BLANKET PURCHASE AGREEMENT (BPA)

GS00T13AJA0024

Continuous Diagnostics and Mitigation (CDM), Tools and Continuous Monitoring as a Service (CMaaS)

in support of:

The U.S. Department of Homeland Security

Issued to:

The Technica Corporation CTA Team

UNDER GSA IT Schedule 70
The Contractor's Basic GSA Schedule contract is applicable to this BPA and any orders issued against it.

Conducted under FAR 8.4 – Federal Supply Schedules

Administered by:
General Services Administration
Federal Systems Integration and Management Center (FEDSIM)
1800 F Street., NW
Suite 3100
Washington, DC 20405

August 12, 2013

FEDSIM Project Number 12083HSM

1.1 ORDER TYPE

The contractor shall perform the effort required by this Blanket Purchase Agreement (BPA) under order(s) on a Labor Hour (LH) and Firm-Fixed-Price (FFP) basis. The work shall be performed in accordance with all sections of this BPA and the offeror's General Services Administration (GSA) Multiple Award Schedule (MAS), under which the resulting order will be placed. An acronym listing to support this Request for Quote (RFQ) is included in Section 9 - Attachment I.

1.2 SERVICES AND PRICES

Long-distance travel is defined as travel over 50 miles. Local travel will not be reimbursed.

The following abbreviations are used in this price schedule:

CLIN Contract Line Item Number
FFP Firm-Fixed-Price
LH Labor-Hour
NSP Not Separately Priced
NTE Not-to-Exceed

This BPA is awarded to all CTA members listed below:

- Technica Corporation (GS-35F-0171V)
- Carahsoft Technology Corporation (GS-35F-0119Y)
- Synnex Corporation (GS-35F-0143R)
- IT Federal Sales, LLC (GS-35F-0494T)
- DLT Solutions, LLC (GS-35F-267DA)
- FedResults, Inc. (GS-35F-0256K)
- ImmixTechnology, Inc. (GS-35F-0265X)
- EC America (GS-35F-0511T)
- Iron Bow Technologies, LLC (GS-35F-0251V)
- Promark Technologies, Inc. (GS-35F-303DA)
- Technical Communities, Incorporated (TCI) (GS-35F-0311R)
- CoreBlox, LLC (GS-35F-018CA)

NOTE: *Regarding CLIN Tables in sections 1.2.1 – 1.2.5. The CLIN tables are provided as an example of a potential CLIN structure for Task Orders placed against this BPA."*

1.2.1 BASE PERIOD

TOOLS CLINs

See Attachment K for tool band pricing. Use the appropriate tab for the corresponding year.

CLIN	Description	Unit of Issue	Unit Price
0001 – Manufacturer Part # (MPN)	Phase 1 Products (HWAM, SWAM, CM, VUL)	ea	$
0002 – Manufacturer Part # (MPN)	Phase 2 products (TFAs 6-9)	ea	$

CLIN	Description	Unit of Issue	Unit Price
0003 – Manufacturer Part # (MPN)	Phase 3 products (TFAs 5, 10-15)	ea	$
0004 RESERVED			

LABOR CLINs

See Attachment L for labor categories and rates. Use the appropriate tab for the corresponding year.

CLIN	Description	Unit of Issue	Hourly Rate
0005	FFP Labor		
0006	LH Labor		
		Hour	$
		Hour	$
		Hour	$

TRAVEL CLIN

CLIN	Description	
0007	Long Distance Travel	Order dependent

1.2.2 OPTION PERIOD 1

TOOLS CLINs

See Attachment K for tool band pricing. Use the appropriate tab for the corresponding year.

CLIN	Description	Unit of Issue	Unit Price
1001 – Manufacturer Part # (MPN)	Phase 1 Products (HWAM, SWAM, CM, VUL)	ea	$
1002 – Manufacturer Part # (MPN)	Phase 2 Products (TFAs 6-9)	ea	$
1003 – Manufacturer Part # (MPN)	Phase 3 Products (TFAs 5, 10-15)	ea	$
1004 RESERVED			

LABOR CLINs

See Attachment L for labor categories and rates. Use the appropriate tab for the corresponding year.

CLIN	Description	Unit of Issue	Hourly Rate
1005	Reserved Labor CLIN		
1006	Labor		
		Hour	$
		Hour	$
		Hour	$

TRAVEL CLIN

CLIN	Description	
1007	Long Distance Travel	Order dependent

1.2.3 OPTION PERIOD 2

TOOLS CLINs

See Attachment K for tool band pricing. Use the appropriate tab for the corresponding year.

CLIN	Description	Unit of Issue	Unit Price
2001 – Manufacturer Part # (MPN)	Phase 1 Products (HWAM, SWAM, CM and VUL)	ea	$
2002 – Manufacturer Part # (MPN)	Phase 2 Products (TFAs 6-9)	ea	$
2003 – Manufacturer Part # (MPN)	Phase 3 Products (TFAs 5, 10-15)	ea	$
2004 RESERVED			

LABOR CLINs

See Attachment L for labor categories and rates. Use the appropriate tab for the corresponding year.

CLIN	Description	Unit of Issue	Hourly Rate
2005	Reserved Labor CLIN		
2006	Labor		
		Hour	$
		Hour	$
		Hour	$

TRAVEL CLIN

CLIN	Description	
2007	Long Distance Travel	Order dependent

1.2.4 OPTION PERIOD 3

TOOLS CLINs

See Attachment K for tool band pricing. Use the appropriate tab for the corresponding year.

CLIN	Description	Unit of Issue	Unit Price
3001 – Manufacturer Part # (MPN)	Phase 1 Products (HWAM, SWAM, CM, VUL)	ea	$
3002 – Manufacturer Part # (MPN)	Phase 2 Products (TFAs 6-9)	ea	$
3003 – Manufacturer Part # (MPN)	Phase 3 Products (TFAs 5, 10-15)	ea	$
3004 RESERVED			

LABOR CLINs

See Attachment L for labor categories and rates. Use the appropriate tab for the corresponding year.

CLIN	Description	Unit of Issue	Hourly Rate
3005	Reserved Labor CLIN		
3006	Labor		
		Hour	$
		Hour	$
		Hour	$

TRAVEL CLIN

CLIN	Description	
3007	Long Distance Travel	Order dependent

1.2.5 OPTION PERIOD 4

TOOLS CLINs

See Attachment K for tool band pricing. Use the appropriate tab for the corresponding year.

CLIN	Description	Unit of Issue	Unit Price
4001 – Manufacturer Part # (MPN)	Phase 1 Products (HWAM, SWAM, CM, VUL)	ea	$
4002 – Manufacturer Part # (MPN)	Phase 2 Products (TFAs 6-9)	ea	$
4003 – Manufacturer Part # (MPN)	Phase 3 Products (TFAs 5, 10-15)	ea	$
4004 RESERVED			

LABOR CLINs

See Attachment L for labor categories and rates. Use the appropriate tab for the corresponding year.

CLIN	Description	Unit of Issue	Hourly Rate
4005	Reserved Labor CLIN		
4006	Labor		
		Hour	$
		Hour	$
		Hour	$

TRAVEL CLIN

CLIN	Description	
4007	Long Distance Travel	Order dependent

1.3 INCREMENTAL FUNDING LIMITATION OF GOVERNMENT'S OBLIGATION

FFP orders must be fully funded upon award. For non-FFP orders, however, the Government, at its discretion, reserves the right to incrementally fund any LH order issued under this BPA. If an order is incrementally funded, it shall specify the total amount of the order, the amount obligated, the estimated performance period based on the amount of obligated funds, and a statement that the contractor is not required to perform work nor is the Government obligated to reimburse the contractor for work performed in excess of the amount obligated.

1.4 AVAILABILITY OF FUNDS

Many Government agencies' operating funds are appropriated for a specific fiscal year. Funds may not be presently available for any orders placed under the BPA or any option year. The Government's obligation on orders placed under this BPA is contingent upon the availability of appropriated funds from which payment for ordering purposes can be made. No legal liability on the part of the Government for any payment may arise until funds are available and until there is written notice to the contractor from the Contracting Officer.

1.5 ESTIMATED PRICES

The aggregate sum of all orders awarded under this BPA (the overall estimated value of this BPA) is $6.0 Billion over a five-year period of performance (assuming all option periods are exercised).

1.5.1 ACQUISITION, CONTRACTING, AND TECHNICAL (ACT) FEE

The Acquisition, Contracting, and Technical (ACT) fee is the cost of awarding, administering, and managing the Continuous Diagnostics and Mitigation (CDM), Tools and Continuous Monitoring as a Service (CMaaS) BPA. The ACT fee for this BPA is 2%, which shall be invoiced as a separate line item at the Order level. This ACT fee is in addition to the Industrial Funding Fee (IFF). This fee applies only to tools and labor and does not apply to travel associated with the respective Orders. Please note the ACT fee does not apply to Orders issued by GSA or DHS.

The contractor shall electronically submit a Report of Sales to the BPA CO and COR, using the format in Section 9 –Attachment M, within 15 days following the completion of the quarterly reporting period, or as requested by the BPA CO. Negative reports are required. The BPA CO and COR will provide written approval of each report. Once approved, the contractor shall submit the ACT fee. Remittance of the ACT fee shall be made by the contractor on a United States Government fiscal year (FY), quarterly basis (e.g., October-December, January-March, April-June, July-September) or as otherwise requested by the BPA Contracting Officer (BPA CO).

ACT fees that have not been paid within 30 calendar days of report approval by the BPA CO shall be considered a debt to the United States Government under the terms of FAR 32.6

Contract Debts. The Government may exercise all its rights under the BPA, including withholding or setting off payments and interest on the debt (see FAR clause 52.232-17, Interest). Failure of the contractor to pay the ACT fee in a timely manner may result in termination of the BPA.

1.5.2 CUMULATIVE VOLUME DISCOUNTS FOR TOOLS

For each tool quoted in the contractor's completed tool price sheet (Section 9 – Attachment K), the contractor shall offer a discounted price off of the GSA Schedule 70 price for each of the bands outlined in Attachment K. To quote orders under this BPA, the contractor shall use the discount band equal to the total (cumulative) volume of device license purchases awarded to the contractor in previous orders under this BPA. Note that "cumulative" refers to volume of license purchases for the total customer base rather than per ordering activity. For purposes of pricing, a device may be a user (actual person), an addressable device on the network, or a removable device.

1.5.3 ADDITIONAL DISCOUNTS

In response to individual order RFQs issued under this BPA, the contractor may (but is not required to) quote additional discounts from the cumulative discounts in Section 1.5.2.

1.6 FFP "AS A SERVICE" PRICING IN ORDERS

It is the Government's intent to implement "as a service" pricing for some orders when appropriate to the Government's requirements. This will be one or more FFP CLINs that will bundle software, ancillary hardware, and services requirements for a defined contract period into one FFP price. The contractor shall then propose one FFP based on hardware, tools, and services as available on contractor's IT Schedule 70 and this BPA. If required, details instructing the contractor to provide pricing for these CLINs will be in the order.

2.1 BACKGROUND

The Department of Homeland Security (DHS) has responsibility for overseeing and assisting Government-wide and agency-specific efforts to provide adequate, risk-based, and cost-effective cybersecurity, per Office of Management and Budget (OMB) Memorandum 10-28.

The cyber landscape in which Federal agencies operate is a constantly changing and dynamic environment. Threats to the nation's information security continue to evolve, and government leaders have recognized the need for a modified approach in protecting our cyber infrastructure. The new approach moves away from historical compliance reporting toward combating threats to our nation's networks on a real time basis. The tools and services delivered through the Continuous Diagnostics and Mitigation (CDM, also known as Continuous Monitoring) program will provide Federal agencies, and state and local governments, with the ability to enhance/automate their existing continuous network monitoring capabilities, correlate and analyze critical security-related information, and enhance risk-based decision making at the agency and Federal enterprise level. Information obtained from the automated monitoring tools will allow for the correlation and analysis of security-related information across the Federal enterprise.

2.1.1 PURPOSE

DHS has been given the authority, and funding for the CDM program to strengthen the cybersecurity posture of the Federal civilian ".gov" networks. By centrally managing and funding this program, DHS will be able to ensure that the approach to continuous monitoring is consistent, meets minimum critical requirements, and leverages centralized acquisition to improve the speed of procurement, and achieve significant discounts by consolidating like Federal requirements into "buying groups." This initiative is also in direct support of the Administration's Cross-Agency Priority (CAP) goal for implementing continuous monitoring across the Federal networks.

While the scope of the program is primarily for civilian ".gov" networks, DHS anticipates use of this BPA by any Federal entity, including Department of Defense (DoD), ".mil" networks, further enhancing the value to the Government of this acquisition.

Finally, in its overall cyber-defense role, DHS has the strategic goal of making the CDM tools and CMaaS available for use by state, local, tribal, and territorial governments. This BPA, through the Cooperative Purchasing Program (CPP), will allow these local entities to benefit from the same consistency, pricing, and speed of procurement for CDM as will be available to Federal entities under this acquisition.

2.1.2 AGENCY MISSION

DHS has a mission to safeguard and secure cyberspace in an environment where the cyber attack threat is continuously growing and evolving. This acquisition will provide DHS with specialized information technology (IT) services and tools to implement DHS' CDM program. This program seeks to defend Federal IT networks from cybersecurity threats by providing continuous monitoring sensors (tools), diagnosis, mitigation tools, and CMaaS to strengthen the security posture of Government networks.

2.2 SCOPE

This acquisition will provide DHS, Federal Government departments / agencies, and state, local, tribal and territorial governments with specialized information technology (IT) services and tools to implement DHS' Continuous Diagnostic and Mitigation (CDM) program. The CDM program seeks to defend Federal and other government IT networks from cyber-security threats by providing continuous monitoring sensors (tools), diagnosis, mitigation tools and Continuous Monitoring as a Service (CMaaS) to strengthen the security posture of Government networks.

Within the scope of the CDM Tools and CMaaS BPA, the contractor shall provide tools and services required by ordering agencies to implement an effective CDM program.

The scope for Tools includes the 15 tool functional areas, as well as providing ancillary hardware as listed in Section 2.2.1.

The scope for CMaaS includes the task areas listed in Section 2.2.2.

For this BPA, the Government uses the term "as a service" within the acronym "CMaaS" to represent the IT professional services required to implement, maintain, and operate CM tools. At the order level, there are two options: Tools and services may be purchased individually or "as a service." However, for the purpose of price evaluation and award of this BPA, the pricing requested is traditional FFP for tools and LH for services. Therefore, this BPA uses the term "CMaaS" to represent all CM IT services regardless of how they are priced or deployed.

2.2.1 SCOPE: TOOLS FUNCTIONAL AREAS

The contractor shall offer tools to perform in the functional areas below, as required to support requirements of individual orders under this BPA.

2.2.1.1 TOOL FUNCTIONAL AREA 1 - HARDWARE ASSET MANAGEMENT

The Hardware Asset Management (HWAM) Function is to discover unauthorized or unmanaged hardware on a network. Once unauthorized or unmanaged hardware is discovered by the contractor's provided tool(s), the agency will take action to remove this hardware. Since unauthorized hardware is unmanaged, it is likely vulnerable and will be exploited as a pivot to other assets if not removed or managed.

2.2.1.2 TOOL FUNCTIONAL AREA 2 - SOFTWARE ASSET MANGEMENT

The Software Asset Management (SWAM) Function is to discover unauthorized or unmanaged software configuration items (SWCI) in IT assets on a network. Once unauthorized or unmanaged SWCI are discovered by the contractor's provided tool(s), the agency will take action to remove these SWCI. Because unauthorized software is unmanaged, it is probably vulnerable to being exploited as a pivot to other IT assets if not removed or managed. In addition, a complete, accurate, and timely software inventory is essential to support awareness and effective control of software vulnerabilities and security configuration settings; malware often exploits vulnerabilities to gain unauthorized access to and tamper with software and configuration settings to propagate itself throughout the enterprise.

2.2.1.3 TOOL FUNCTIONAL AREA 3 - CONFIGURATION MANAGEMENT

The Configuration Management (CM) Function is to reduce misconfiguration of IT assets, including misconfigurations of hardware devices (to include physical, virtual, and operating system) and software. Once a misconfiguration of hardware devices is discovered by the contractor provided tools, the supported department / agency will be responsible to take any needed action to resolve the problem or accept the risk. Over 80% of known vulnerabilities are attributed to misconfiguration and missing patches. Cyber adversaries often use automated computer attack programs to search for and exploit IT assets with misconfigurations, especially for assets supporting Federal agencies, and then pivot to attack other assets.

2.2.1.4 TOOL FUNCTIONAL AREA 4 – VULNERABILITY MANAGEMENT

The Vulnerability Management (VUL) Function is to discover and support remediation of vulnerabilities in IT assets on a network. Vulnerability management is the management of risks presented by known software weaknesses that are subject to exploitation. The vulnerability management function ensures that mistakes and deficiencies are identified. Once the contractor provided tool(s) identify these mistakes and deficiencies, the agency will take action to remove or remediate these from operational systems so that they can no longer be exploited. (An information security vulnerability is a deficiency in software that can be directly used by a hacker to gain access to a system or network.).

2.2.1.5 TOOL FUNCTIONAL AREA 5 – MANAGE NETWORK ACCESS CONTROLS

The Manage Network Access Controls (NAC) Function is to prevent, and allow the agency to remove and limit, unauthorized network connections/access to prevent attackers from exploiting internal and external network boundaries and then pivoting to gain deeper network access and/or capture network resident data in motion or at rest. Boundaries include firewalls as well as encryption (virtual private networks). Additionally, the function will prevent, remove, and limit unauthorized physical access.

2.2.1.6 TOOL FUNCTIONAL AREA 6 – MANAGE TRUST IN PEOPLE GRANTED ACCESS

The Manage Trust in People Granted Access (TRU) Function is to prevent insider attacks by carefully screening new and existing persons granted access for evidence that access might be abused. The Manage Trust in People Granted Access capability informs the Manage Account Access (Section 2.2.1.9) capability by providing background information and potential risk, or compromise, factors. These factors are used to determine if someone should be granted access, under the Manage Account Access capability, to certain resources (e.g., sensitive data).

2.2.1.7 TOOL FUNCTIONAL AREAS 7 – MANAGE SECURITY RELATED BEHAVIOR

The Manage Security Related Behavior (BEH) Function is to prevent general users from taking unnecessary risks to prevent attackers from exploiting network and application users via social engineering scams. BEH prevents users with elevated privileges and special security roles from taking unnecessary risks to prevent attackers from exploring poor engineering and/or remediation. The Manage Security Related Behavior capability addresses the behavior of

someone who has been granted access to information technology devices and systems. Information from this capability feeds into the Manage Trust in People Granted Access capability (Section 2.2.1.6) where determinations will be made about someone's suitability for continued access based, in part, on their behavior.

2.2.1.8 TOOLS FUNCTIONAL AREA 8 – MANAGE CREDENTIALS AND AUTHENTICATION

The Manage Credentials and Authentication (MCA) Function is to prevent a) the binding of credentials to or b) the use of credentials by other than the rightful owner (person or service) by careful management of credentials, preventing attackers from using hijacked credentials to gain unauthorized control of resources, especially administrative rights. The MCA capability ensures that account credentials are assigned to, and used by, authorized people. This capability will rely on the results of the Manage Account Access capability (Section 2.2.1.9) to ensure that only trusted people receive credentials. This covers credentials for physical and logistical access.

2.2.1.9 TOOLS FUNCTIONAL AREA 9 – MANAGE ACCOUNT ACCESS

The Manage Account Access (MAA) Function is to prevent access beyond what is needed to meet business mission by limiting account access and eliminating unneeded accounts to prevent attackers from gaining unauthorized access to sensitive data. The Manage Account Access capability will assign access to computing resources based, in part, on their level of trustworthiness (as determined in Functional Area 6, Section 2.2.1.6).

2.2.1.10 TOOLS FUNCTIONAL AREA 10 – PREPARE FOR CONTINGENCIES AND INCIDENTS

The Prepare for Contingencies and Incidents (CP) Function is to prevent loss of confidentiality, integrity, and/or availability by being prepared for unanticipated events and/or attacks that might require recovery and/or special responses, preventing attacker's compromises from being effective by adequate recovery as needed, and natural events from causing permanent loss by adequate preparation as needed.

2.2.1.11 TOOLS FUNCTIONAL AREA 11 – RESPOND TO CONTINGENCIES AND INCIDENTS

The Respond to Contingencies and Incidents (INC) Function is to prevent repeat of previous attacks and limit the impact of ongoing attacks by using forensic analysis, audit information, etc. to a) appropriately respond to end ongoing attacks and to b) identify ways to prevent recurrence to prevent attackers from maintaining ongoing attacks and exploiting weaknesses already targeted by others.

2.2.1.12 TOOLS FUNCTIONAL AREA 12 – DESIGN AND BUILD IN REQUIREMENTS POLICY AND PLANNING

The Design and Build in Requirements Policy and Planning (POL) Function is to prevent exploitation of the system by consciously designing the system to minimize weaknesses and building the system to meet that standard in order to reduce the attack surface and increase the effort required to reach the parts of the system that remain vulnerable. The Design and Built in -

Requirements, Policy, and Planning capability includes software assurance best practices to ensure that security is built into the System Development Lifecycle. This capability addresses how to avoid or remove weaknesses and vulnerabilities before the system is released into production caused by poor design and insecure coding practices.

2.2.1.13 TOOLS FUNCTIONAL AREA 13 – DESIGN AND BUILD IN QUALITY

The Design and Build in Quality (QAL) Function is to prevent attackers from exploiting weaknesses by finding and prioritizing weaknesses and fixing the most important weaknesses first. This capability addresses software before it is installed and operational.

2.2.1.14 TOOLS FUNCTIONAL AREA 14 – MANAGE AUDIT INFORMATION

The Manage Audit Information (AUD) Function is to prevent persistent attacks and weaknesses by using audit information to identify them and initiate an appropriate response. The function addresses agency efforts to monitor the behavior of employees (for example, downloading pornography, unusual times/volumes of access, etc.). The results of these audits feed into the Manage Trust in People Granted Access (Section 2.2.1.6) capability where determinations will be made about someone's suitability for continued access based, in part, on their behavior.

2.2.1.15 TOOLS FUNCTIONAL AREA 15 – MANAGE OPERATION SECURITY

The Manage Operation Security (OPS) Function is to prevent attackers from exploiting weaknesses by using functional and operational control limits to help senior managers determine when to authorize operation of systems, and when to devote extra attention to reducing risks to prevent attackers from exploiting preventable weaknesses and analyze prior failures to identify and resolve system weaknesses. This activity receives information from the Manage Audit/Information (Section 2.2.1.14) capability to help support leadership decisions to enable improvement of security. It covers information about all operational capabilities and, therefore, does not apply to the creation of a system.

2.2.1.16 PROVIDE ANCILLARY HARDWARE

When required by orders under this BPA, the contractor shall provide ancillary IT hardware as needed to support the operation of the contractor's CDM Tool(s). All ancillary IT hardware must be on the contractor's GSA Schedule 70 contract or, in the event of a Contractor Teaming Arrangement (CTA), the contract of a teaming partner. The Government may allow the offeror to add a Contractor Teaming member after award if the Contracting Officer determines that it is in the best interest of the Government.

2.2.2 CMAAS TASK AREAS

The contractor shall provide functional, strategic, and managerial business consulting and support services in the execution of the overall program missions. Activities to be supported under this BPA by orders are described below:

Unless stated otherwise in the RFQ under this BPA, at the order level, the Government will provide specific requirements regarding the target IT environment for the agency or organization for which CMaaS is required, in sufficient detail that the provider can determine the number and

type of assets for which sensors need to be provided and the frequency of data collection (e.g., asset discovery, vulnerability scanning) required by the requesting organization. Subject to specific order requirements, the baseline number of IT assets may be provided based on a preliminary asset inventory conducted by the Government using its own non-commercial discovery tool. The order request will also specify any existing sensor tools, dashboards, or other applications or data sources (i.e., already installed and in operation by the requesting organization) that the CMaaS provider must integrate in its proposed solution architecture, as well as any unique security requirements.

2.2.2.1 CMAAS TASK AREA 1 – PROVIDE ORDER PROJECT MANAGEMENT SUPPORT

The contractor shall provide all necessary personnel, administrative, financial, and managerial resources necessary for the support of order accomplishment. This includes the management and oversight of its performance of the order under the BPA and work performed by contractor personnel, including subcontractors and teaming arrangements/partners, to satisfy the requirements identified in the orders. The contractor should note that adding labor categories is permissible.

The contractor shall provide this support in accordance with the terms and requirements of this BPA and the specific requirements of the order.

Examples of support:

a. Coordinate a Program Kickoff Meeting.
b. Prepare a Monthly Status Report (MSR) at the BPA and order levels.
c. Convene technical status meetings.
d. Prepare project management documentation such as a project management plan (PMP), staffing plan, project schedule, and work breakdown structure (WBS).
e. Manage contractor personnel assigned to the order.
f. Prepare trip reports.
g. Prepare problem notification reports.
h. Notify the Contracting Officer (CO), the Contracting Officer Representative (COR), and Order Government Technical Point of Contact (TPOC) of any technical, financial, personnel, or general managerial problems encountered throughout the BPA and individual orders.
i. Develop and deliver detailed project plans for each order.
j. Evaluate orders under this BPA using Earned Value Management (EVM), where required.

2.2.2.2 CMAAS TASK AREA 2 – CDM ORDER PLANNING

The contractor shall provide plans describing their proposed approach to implement the specific CDM capabilities required by the order. The contractor shall also participate in and /or facilitate technical design reviews consistent with agency system engineering or development lifecycle (SDLC) requirements. The goal of the Order Planning activity is to demonstrate understanding of the requirements by providing sufficiently detailed plans to ensure successful implementation and operation of the CDM capabilities. The contractor shall provide the following documentation under this sub-activity.

a. Proposed CMaaS System Implementation Architecture, showing sensors, dashboards, and connectivity.
b. Draft Security Accreditation package, describing the contractor's plan for implementing required security controls and its security model to prevent cross-propagation of malware across requesting organizations.
c. Proposed Concept of Operations, describing how the proposed architecture will meet the CMaaS requirements for the agency or community of agencies requesting services.
d. Plan for Transition to Production Operations from the existing architecture, including integrating existing tools and dashboards, if requested in the request for quote.
e. Plan for Production Operations, describing how the provider will operate the proposed architecture to meet CDM objectives.
f. Plan for Governance Support, describing how the provider will assist cooperating agencies to establish and coordinate governance of the CMaaS solution.
g. Requirements for any Government-Furnished Equipment/Government-Furnished Services on which the provider is relying to meet the CMaaS objectives.
h. Perform "as is" analysis on agency existing infrastructure to facilitate better CDM program and IT architecture planning.

2.2.2.3 CMAAS TASK AREA 3 – SUPPORT CDM DASHBOARDS

The contractor shall provide the technical services necessary to install, configure, and maintain the envisioned DHS-provided Base CDM dashboard, any Intermediate (Summary or Object-level) dashboards, or other agency-supplied dashboard or CDM reporting systems, for use by requesting organizations. The CDM dashboard function includes dashboards at different levels of the CDM architecture. These include "Top," "Intermediate," and "Base" dashboards, which may be further categorized as "Summary" or "Object-level" (as shown in Section 9 –Attachment O). The contractor shall all perform all appropriate quality assurance and technical testing to ensure the delivered tools perform to the requirements specified in the order.

2.2.2.4 CMAAS TASK AREA 4 – PROVIDE-SPECIFIED TOOLS AND SENSORS

The contractor shall provide, install and configure a suite of CDM tools (as specified in an order) to perform / support the tool functional areas specified in Section 2.2.1: Hardware Inventory Management, Software Inventory Management, Configuration Setting Management, Vulnerability Management, Network and Physical Access Management, Trust Condition Management, Management of Security Related Behavior, Credentials and Authentication Management, Account Access Management, Contingency and Incident Preparation, Contingency and Incident Response, Design and Build in Requirements, Policy, and Planning, Design and Build in Quality, Operational Audit Information Management, Operational Security Management, and Management of other tools and sensors. If required by an order, these tools may include open source / public license software. In order to perform this task, orders may require the contractor to also provide, install, and configure ancillary IT hardware if needed to support the operation of the provided CDM tools. The contractor shall also perform all appropriate quality assurance and technical testing to ensure the delivered tools perform to the requirements specified in the order.

2.2.2.5 CMAAS TASK AREA 5 – CONFIGURE AND CUSTOMIZE TOOLS AND SENSORS

The contractor shall, according to the requirements of the requesting organization, customize the sensors and tools to accomplish the objective of assessing, for each capability, any deviations between the desired state of the IT asset and the actual state of the asset. This customization shall include the capability for the requesting agency to (1) record the desired state for authorized assets, (2) specify its own categories for grouping results, (3) customize scoring algorithms to quantify results, (4) customize grading standards for defect scores, and (5) establish responsibility for maintaining the desired state (and mitigating defects) of each assigned and discovered asset. Customization of software may include requirements to localize tools when required by an order. The contractor shall also perform all appropriate quality assurance and technical testing to ensure the delivered tools perform to the requirements specified in the order.

2.2.2.6 CMAAS TASK AREA 6 – MAINTAIN DATA ON DESIRED STATE FOR CDM TOOLS AND SENSORS

The contractor shall provide operational capability for the installed and configured tools and sensors that enables agencies to keep the data current for the desired state of target IT assets (baseline data), as needed, and on an ongoing basis.

2.2.2.7 CMAAS TASK AREA 7 – OPERATE CDM TOOLS AND SENSORS

The contractor shall operate the installed suite of CDM sensors to determine and report the actual state for functions within the periodicity specified in the order: Hardware Inventory Management, Software Inventory Management, Configuration Setting Management, Vulnerability Management, Network and Physical Access Management, Trust Condition Management, Management of Security Related Behavior, Credentials and Authentication Management, Account Access Management, Contingency and Incident Preparation, Contingency and Incident Response, Design and Build in Requirements, Policy, and Planning, Design and Build in Quality, Operational Audit Information Management, Operational Security Management, and Management of other tools and sensors. If defined in order requirements for supported agencies, the contractor shall also remove and remediate threats that are detected by the CDM tools and sensors. The contractor shall also perform all work necessary to maintain and provide end software support to the tools and any ancillary hardware; including patching, upgrades, end-user support and replacement of failed components.

2.2.2.8 CMAAS TASK AREA 8 – INTEGRATE AND MAINTAIN INTEROPERABILITY BETWEEN CDM TOOLS AND AGENCY LEGACY APPLICATIONS AND DATA

The contractor shall integrate CDM-operated tools and dashboard with associated agency information systems (as specified in the order) and maintain interoperability between the CDM tools and the agency data in operation. (For example, an agency might want to have data feeds exchanged between their existing property management system and the HWAM infrastructure.) The contractor shall also perform all appropriate quality assurance and technical testing to ensure the delivered tools perform to the requirements specified in the order.

2.2.2.9 CMAAS TASK AREA 9 – OPERATE DATA FEEDS TO AND FROM INSTALLED DASHBOARDS

The contractor shall operate the DHS-provided dashboard to provide data feeds from the tools and sensors operated under Section 2.2.2.8 to the appropriate Intermediate dashboard(s) and any requested rollup (Summary or Object) dashboards (see Section 9 –Attachment O). The contractor shall operate data feeds between each operated dashboard and its parent dashboard. The contractor shall send data from the requesting organization's own summary dashboard (if installed and required by the order) to the DHS-provided dashboard. The contractor shall send data from the console of an existing sensor (if installed and required by the order) to the DHS-provided dashboard. The contractor shall also provide the agency with a capability to retain all data within the agency-specified data retention criteria, if required by the requirements of an order. The contractor shall also perform all appropriate quality assurance and technical testing to ensure that data feeds perform to the requirements specified in the order.

2.2.2.10 CMAAS TASK AREA 10 – TRAINING AND CONSULTING IN CDM GOVERNANCE FOR DEPARTMENTS, AGENCIES, AND OTHER REQUESTING ORGANIZATIONS

The contractor shall provide training and/or consulting to agencies and other requesting organizations to assist them in establishing an overall cybersecurity governance program with emphasis on using the continuous diagnostics to perform the most cost-effective mitigations within available resources. Training and consulting tasks are expected to include support for agency activities including, but not limited to:

a. Identification of and communication with stakeholders.
b. Assessing risk/priorities and agency readiness for transition.
c. Assist the Government with designing Federal scoring/grading to compare performance and progress of agencies to:
    1. Ensure fairness and transparency in assessment, scoring, and grading.
    2. Ensure validity and reliability in assessment, scoring, and grading.
d. Conducting No-Fault "Pilot" operation phase and transition from pilot to full operation.
e. Conducting Federal-level decision boards to:
    1. Assign and transfer risk conditions.
    2. Manage new or newly discovered risks.
    3. Coordinate with US Computer Emergency Response Team (US-CERT), DHS' National Cyber Security Division (NCSD), etc.
    4. Resolve configuration management issues.
    5. Measure and manage sensor performance.
    6. Resolve dashboard performance/usability issues (e.g., false positives, false negatives).
    7. Coordinate standards and policies.
f. Providing agency manager assistance, such as:
    1. Rollout Tiger Teams.
    2. Help Desk support.
    3. User group management.
    4. Website to provide automated assistance/reference.

g. Assistance with Security Assessment and Authorization (formerly Certification and Accreditation) such as:
    1. Models for using CDM results in ongoing Assessment and Authorization.
    2. Models for using dashboards to meet plan of action and milestone (POA&M) requirements.
h. Coordination with agency office of inspector general (OIG) or Government Accounting Office (GAO) to support agency with audit compliance.
i. Establishing and maintaining an overall cybersecurity governance plan.
j.) Other governance activities identified by DHS and/or agencies.

2.2.2.11 CMAAS TASK AREA 11 – SUPPORT INDEPENDENT VERIFICATION & VALIDATION (IV&V) AND SYSTEM CERTIFICATION

The contractor shall provide the necessary engineering, project management, data, and documentation to support independent verification and validation (IV&V) efforts by third parties or Government personnel to accept / certify system or other deliverables as required by the order.

This Page is Intentionally Left Blank

4.1 PLACE OF INSPECTION AND ACCEPTANCE

Inspection and acceptance of all work performance, reports, and other deliverables under this BPA, shall be defined in individual orders.

4.2 SCOPE OF INSPECTION

All deliverables will be inspected for content, completeness, accuracy, and conformance to order requirements by the COR as defined in the order. Inspection may include validation of information or software through the use of automated tools, testing, or inspections of the deliverables, as specified in the order. The scope and nature of this inspection will be sufficiently comprehensive to ensure the completeness, quality, and adequacy of all deliverables. Prior to delivery of systems and software, the contractor may be required to support independent contractor or Government observation of any or all contractor inspections as defined in the order. Additionally, any inspection events may be used for pre-planned data collection and independent contractor or Government evaluation as defined in the order.

The time period required, the necessary contractor documentation and reports, and method the Government will use to inspect deliverables, will be defined by individual orders under this BPA.

4.3 BASIS OF ACCEPTANCE

The basis for acceptance shall be compliance with the requirements set forth in the individual order under this BPA, the contractor's quote and relevant terms and conditions of the contract. Deliverable items rejected shall be corrected in accordance with the applicable clauses.

Reports, documents, and narrative-type deliverables will be accepted when all discrepancies, errors, or other deficiencies identified in writing by the Government have been corrected.

If the draft deliverable is adequate, the Government may accept the draft and provide comments for incorporation into the final version.

All of the Government's comments on deliverables must either be incorporated in the succeeding version of the deliverable, or the contractor must demonstrate to the Government's satisfaction why such comments should not be incorporated.

If the Government finds that a draft or final deliverable contains spelling errors, grammatical errors, or improper format, or otherwise does not conform to the requirements stated within the specific order requirements, the document may be immediately rejected without further review and returned to the contractor for correction and resubmission. If the contractor requires additional Government guidance to produce an acceptable draft, the contractor shall arrange a meeting with the COR.

4.3.1 INFORMATION TECHNOLOGY (IT) ACCEPTANCE

For IT solutions, including configuration and development, the final acceptance will occur when all discrepancies, errors, or other deficiencies identified in writing by the Government have been resolved through documentation updates, program correction, or other mutually agreeable methods.

4.4 DRAFT DELIVERABLES

The Government will provide written acceptance, comments, and/or change requests to any draft deliverables within ten workdays of receipt of the draft deliverable unless another time period is specified in the individual order.

Unless another time period is specified in the individual order, the contractor shall have ten workdays to incorporate the Government's comments and/or change requests and to resubmit the deliverable in its final form.

4.5 WRITTEN ACCEPTANCE/REJECTION BY THE GOVERNMENT

The order CO /COR will provide written notification of acceptance or rejection of all final deliverables within ten workdays of receipt of the final deliverable unless another time period is specified in the individual order. All notifications of rejection will be accompanied with an explanation of the specific deficiencies causing the rejection.

4.6 NON-CONFORMING PRODUCTS OR SERVICES

Non-conforming products or services will be rejected. Deficiencies will be corrected, by the contractor, within ten workdays of the rejection notice. If the deficiencies cannot be corrected within ten workdays, the contractor shall immediately notify the order COR of the reason for the delay and provide a proposed corrective action plan within ten workdays.

5.1 PERIOD OF PERFORMANCE

The period of performance for this BPA is a one-year base period and four, one-year options from date of award (total five years). An offeror, whether prime contractor or CTA may be awarded a BPA that extends beyond the current term of its GSA Schedule contract, so long as there are option periods in the GSA Schedule contract that, if exercised, will cover the BPA's entire ordering period. Each order issued under this BPA will specify a period of performance for the order. Orders under this BPA will not have a period of performance that exceeds the BPA period of performance by more than one year. Orders issued there under this BPA cannot be transferred to another GSA Schedule 70 contract. In the event a CTA Team Lead is removed or the Team Lead's GSA Schedule 70 contract has expired and additional option periods not exercised, a new Team Lead must be designated in order for the BPA to continue. In the event a prime contractor in a prime/sub arrangement loses its Schedule 70 contract, the BPA will not continue.

5.2 PLACE OF PERFORMANCE

The place of performance will be defined in the individual order issued under this BPA. Long-distance and overseas travel may be required to perform work under an individual order and will be detailed within the order if required.

5.3 ORDER SCHEDULE AND MILESTONE DATES

Deliverables and milestones will be specified with the individual orders.

5.4 PUBLIC-RELEASE OF CONTRACT DOCUMENTS REQUIREMENT

For all orders issued under this BPA by GSA FEDSIM, the contractor agrees to submit, within ten workdays from the date of the CO's execution of the initial BPA, or any order, or any modification to these documents (exclusive of Saturdays, Sundays, and Federal holidays), a portable document format (PDF) file of the fully executed document with all proposed necessary redactions, including redactions of any trade secrets or any commercial or financial information that it believes to be privileged or confidential business information, for the purpose of public disclosure at the sole discretion of GSA. The contractor agrees to provide a detailed written statement specifying the basis for each of its proposed redactions, including the applicable exemption under the Freedom of Information Act (FOIA), 5 U.S.C. § 552, and, in the case of FOIA Exemption 4, 5 U.S.C. § 552(b) (4), shall demonstrate why the information is considered to be a trade secret or commercial or financial information that is privileged or confidential. Information provided by the contractor in response to the contract requirement may itself be subject to disclosure under the FOIA. Submission of the proposed redactions constitutes concurrence of release under FOIA.

GSA will carefully consider all the contractor's proposed redactions and associated grounds for nondisclosure prior to making a final determination as to what information in such executed documents may be properly withheld.

5.5 DELIVERABLES MEDIA

Unless specified otherwise in the order, the contractor shall deliver all electronic versions by email and removable electronic media, as well as placing the deliverables in any designated repository. Unless specified otherwise in an order, the following are the required electronic formats, whose versions must be compatible with the latest, commonly available version on the market.

- Text MS Word
- Spreadsheets MS Excel
- Briefings MS PowerPoint
- Drawings MS Visio
- Schedules MS Project

5.6 PLACE(S) OF DELIVERY

Unclassified deliverables or correspondence shall be delivered to the Order CO or COR at the address specified in the order.

5.7 NOTICE REGARDING LATE DELIVERY/ PROBLEM NOTIFICATION

The contractor shall notify the Ordering CO / COR, using procedures outlined in the individual order, as soon as it becomes apparent to the contractor that a scheduled delivery will be late. The contractor shall include in the notice, the rationale for late delivery, the expected date for the delivery, and the project impact of the late delivery. The Ordering COR will review the new schedule and provide guidance to the contractor. Such notification in no way limits any Government contractual rights or remedies including, but not limited to, termination.

5.8 MARKETING

The contractor may "market" and advertise this BPA to Federal, state, local, tribal, and territorial government IT staff, departments, and agencies. Possible actions include: advertising resultant BPA on the vendor's website, advertising the agreement at relevant trade shows, and participation in GSA/FEDSIM and DHS sponsored events and discussion with news media targeted toward potential users of the BPA.

5.8.1 PRESS RELEASE

The contractor may submit a press release for any work awarded against the BPA. The contractor shall provide a draft press release to the Government for review and approval prior to making an official announcement. The draft press release shall be submitted to the CDM@gsa.gov mailbox.

6.1 CONTRACTING OFFICER'S REPRESENTATIVE (COR)

The BPA CO will appoint a BPA COR in writing for the BPA using a COR Appointment Letter that will be provided to the contractor upon award (Section 9 – Attachment A). The BPA COR will provide no supervisory or instructional assistance to contractor personnel.

At the order level, the CO awarding each order under this BPA (referred to as the Order or Ordering CO), may appoint a COR (referred to as the Order or Ordering COR) in writing for that order through a COR Appointment Letter that will be provided to the contractor upon award of the order (the Ordering CO may use the format in Section 9 - Attachment A, or another format specified in the order RFQ). The Ordering COR will receive, for the Government, all work called for by the order and will represent the Ordering CO in the technical phases of the work. The Ordering COR will provide no supervisory or instructional assistance to contractor personnel.

The BPA or Ordering CORs are not authorized to change any of the terms and conditions, scope, schedule, and price of the BPA or the order. Changes in the scope of work will be made only by the Ordering CO by properly executed modifications to the order, or by the BPA CO, by modification to the BPA.

6.1.1 CONTRACT ADMINISTRATION

For the BPA, the following CO is responsible for contract administration

Contracting Officer:

John Terrell
GSA FAS AAS FEDSIM
1800 F Street. NW
Suite 3100
Washington, DC 20405
Telephone: (703) 605-2748
Email: john.terrell@gsa.gov

BPA Contracting Officer's Representative:

Kyle Harrer
GSA FAS AAS FEDSIM
1800 F Street NW
Suite 3100
Washington, DC 20405
Telephone: (202) 372-5192
Email: kyle.harrer@gsa.gov

DHS Technical Point of Contact (TPOC)

John M. Hartman
DHS, Office of Cyber Security
and Communications (CS&C)
Federal Network Resilience
4601 North Fairfax Drive
Arlington, VA 22201
Telephone: (202) 412 – 1083
Email: matthew.hartman@hq.dhs.gov

James J. Quinn
DHS, Office of Cyber Security and Communications (CS&C)
Federal Network Resilience
4601 North Fairfax Drive
Arlington, VA 22201
Telephone: (703) 235 – 4243
Email: jim.quinn@hq.dhs.gov

Individual Orders under this BPA, will designate an Ordering CO and an Ordering COR and a TPOC for that order.

6.2 BPA ORDER ORDERING GUIDELINES

Any department or agency of the Federal Government, or any entity that may use GSA IT Schedule 70, may order from this BPA. Prior to the release of any Order solicitations, the Ordering Contracting Officer (OCO) of any department of agency of the Federal Government must request a Delegation of Procurement Authority.

In addition, state, local, regional, and tribal governments that may use Schedule 70 through the Cooperative Purchasing Program may also use this BPA. Prior to the release of any Order solicitations, the Ordering Contracting Officer (OCO) of any state, local, regional, and tribal governments, and those authorized by state, local and tribal entities to compete, award, and administer Orders on behalf of those entities must request a Memorandum for Ordering Contracting Officer (MOCO).

6.2.1 DELEGATION OF PROCUREMENT AUTHORITY (DPA) AND MEMORANDUM FOR ORDERING CONTRACTING OFFICERS

For non-FEDSIM issued orders, a Federal department or agency OCO must request a DPA from the BPA CO (see Section 6.1.1 above) prior to issuing an order solicitation. Only those that have received a DPA may place Orders under this Blanket Purchase Agreement (BPA). The ordering

CO shall request a DPA by submitting a written request to the CDM@gsa.gov mailbox. This request shall include a copy of the ordering CO's warrant for approval.

For non-FEDSIM issued orders, the OCO of any state, local, regional, and tribal governments, and those authorized by state, local and tribal entities to compete, award, and administer Orders on behalf of those entities must request a Memorandum for Ordering Contracting Officer (MOCO) from the BPA CO (see Section 6.1.1 above) prior to issuing an order solicitation. Only those that have received a MOCO may place Orders under this Blanket Purchase Agreement (BPA). The ordering CO shall request a MOCO by submitting a written request to the CDM@gsa.gov mailbox. This request shall include a copy of the ordering CO's valid warrant authority or authorized purchasing agent authority for state, local, regional and tribal entities in accordance with applicable laws, regulations and policies for approval.

6.2.2 ORDER SOLICITATION AND AWARD

Prior to the release of the Order solicitation, the Ordering Contracting Officer (OCO) is required to notify the BPA COR of the estimated dollar value of the Order, as well as Provide Sections 1 and 2 of the RFQ, Order and Supplies and Statement of Work. This allows the BPA COR to track the estimated value of the new order against the cumulative awarded ceiling and validate sufficient BPA ceiling is available. In addition, by providing Sections 1 and 2, the BPA COR will be able to provide the OCO with the necessary tiered price bands for evaluation of the quotes.

Prior to making an order award, the Ordering CO must contact the BPA CO (see Section 6.1.1 above). This will ensure the order value is within the total BPA value, volume discounts are being properly applied, and to answer any questions of scope or modification. All Orders issued against this BPA must be pursuant to FAR 8.405 – 3(c)(2).

Zero or more orders may be issued during the performance period of this BPA; it is understood and agreed that the Government has no obligation to issue orders. The contractor agrees to accept and perform orders issued by a CO from any department or agency of the Federal Government within the scope of this agreement. Contractor acceptance of orders from state, local, regional, and tribal governments is voluntary. In the event of a conflict between an order, the BPA, or the contractor's GSA Schedule contract, the GSA Schedule contract takes precedence.

6.2.2.1 ORDER REQUEST FOR QUOTE (RFQ) SUBMISSION

Each individual RFQ may be LH, FFP, or any combination of the two. For any order that is other than FFP, the ordering activity shall include, at a minimum, the documentation outlined in FAR 8.405-2(e). The RFQ may include specific metrics and quality assurance methods (if applicable).

All RFQs will incorporate all terms and conditions of the BPA. In addition, the proposed RFQ will include the following to the extent applicable to individual orders:

a. A Statement of Work (SOW) or other performance-based work statement describing the work to be performed, the deliverables, the period of performance, Government Points of Contact (POCs), description of marking information, data rights, inspection and

acceptance of services, security requirements, and Government-Furnished Information / Property, as applicable.
b. The submission date/time and the method of delivery for quotes.
c. Specific instructions on what to include in the quote submission. This may include, but is not limited to, written responses summarizing technical and price approaches.
d. Evaluation factors.
e. Other information deemed appropriate.

6.2.2.2 ORDER QUOTE SUBMISSION

Quote response time will be determined at the ordering level and outlined in the solicitation. At a minimum the quote shall include:

a. **Price:** The quote may include a detailed cost per hour of all labor required to accomplish the tasks as set forth in the RFQ, or be a fixed-price quote with sufficient information to substantiate the price quoted. At a minimum, pricing shall be the BPA pricing in accordance with Section 1 – Supplies or Services and Price/Costs, including cumulative price discounts for tools. The BPA Team (Leader / Member(s)) or prime contractor shall provide off-site or on-site rates as required by the order. The discounts offered do not preclude the CTA Team or the prime contractor from offering or the Government requesting, further price reductions in accordance with commercial practices, market forces, and volume buying at the time of placing orders.

b. **Statement disclosing any known or expected conflicts of interest pursuant to FAR 9.5:** The quote may also require the submission of the following information (the Government is not limited to the below list and may require other information):

    1. Technical information (e.g., technical approach, including team partners and experience as required by the RFQ).
    2. Technical data, computer software, and computer software documentation, if applicable, as required in reference to meeting the needs of the statement of work in the RFQ.
    3. Corporate Experience (as it relates to the specific requirements of an order).
    4. Proposed Key Personnel and Staffing.
    5. Price Quote and any additional discounts against the schedule labor rates.

c. **Evaluation:** The Government will evaluate responses against evaluation criteria contained in the order RFQ.

6.2.2.3 ORDER ISSUANCE

The SOW, labor mix, and hours (if applicable), as well as a proposed ceiling price for the RFQ, may be incorporated into any order. The proposed technical solution may also be incorporated in the order. At any time during the duration of the BPA, the BPA CO reserves the right to revise the procedures pertaining to order issuance. Contracting Officers from entities that have the right to utilize GSA Schedule 70 are the only individuals that are authorized to issue orders and obligate the Government for orders awarded under the BPA. Each order shall, as appropriate:

a. Set forth a pricing schedule.
b. Set forth the specific level of effort and/or performance outcomes desired to be fulfilled under the order based on the estimated dollar value and complexity of the proposed order.
c. Designate the Ordering COR who will perform inspection and acceptance.
d. Set forth any payment options.
e. Be dated.
f. Set forth the property, if any, to be furnished by the Government and the date(s) such property is to be delivered to the contractor.
g. Set forth the disbursing office where payment is to be made.
h. Set forth administration data.
i. Set forth the contractor's and Government's respective technical data rights.
j. Set forth any other pertinent information
k. Unauthorized Work: The contractor is not authorized to commence order performance prior to issuance of an awarded order.
l. Order Funding Restrictions: No unfunded orders are allowed.
m. Ordering Period: Orders for services specified in Section 2 of the BPA may be issued by the Ordering CO within the ordering period of the BPA.
n. Responsibilities of the Ordering CO: A copy of all pricing shall be provided to the BPA CO in order to ensure the price ceiling under the BPA is not exceeded.

6.3 INVOICE REQUIREMENTS

6.3.1 GSA FEDSIM-ISSUED ORDER INVOICE REQUIREMENTS

For orders issued by GSA FEDSIM, if no payment schedule is specified in the order the following applies.

The Government desires that the final invoice be submitted by the contractor within six months of project completion.

All invoices shall list the Data Universal Numbering Systems (DUNS) number, BPA Number and order number.

6.3.1.1 LABOR HOUR (LH) CLINs

The contractor may invoice monthly on the basis of hours incurred for the LH CLINs. The invoice shall include the period of performance covered by the invoice and the CLIN number and title. All hours shall be reported by CLIN element (as shown in Section 1 – Supplies or Services and Price), by contractor employee, and shall be provided for the current billing month and in total from project inception to date. The contractor shall provide the invoice data in spreadsheet form with the following detailed information. The listing shall include separate columns and totals for the current invoice period and the project to date.

a. Employee name (current and past employees)
b. Employee labor category
c. Monthly and total cumulative hours worked
d. Amount billed thus far

6.3.1.2 FIRM-FIXED-PRICE (FFP) CLINs

If no payment schedule is specified in the order, the contractor may invoice on a monthly basis, the amount obtained by dividing the FFP amount for the order period, by the number of months of performance in the period. For FFP CLINs, the invoice shall include the period of performance period covered by the invoice, and the CLIN number and title. All amounts invoiced shall be reported by CLIN element (as shown in Section 1 – Supplies or Services and Price of the order) and shall be provided for the current invoice and in total from project inception to date. The contractor shall provide the invoice data in spreadsheet form with the following detailed information. The listing shall include separate columns and totals for the current invoice period and the project to date.

a. FFP period of performance period – as stated in Section 1 – Supplies or Services and Price of the order.
b. Amount invoiced

6.3.1.3 TRAVEL

The contractor may invoice monthly on the basis of cost incurred for cost of travel comparable with the Joint Travel Regulation (JTR)/Federal Travel Regulation (FTR). The invoice shall include the period of performance covered by the invoice, the CLIN number and title, and the IA number. Separate worksheets, in MS Excel format, shall be submitted for travel.

CLIN/Task Total Travel: This invoice information shall identify all cumulative travel costs billed by CLIN/Task. The current invoice period's travel details shall include separate columns and totals and include the following:

a. Travel Authorization Request identifier, approver name, and approval date
b. Current invoice period
c. Names of persons traveling
d. Number of travel calendar days
e. Dates of travel
f. Number of calendar days per diem charged
g. Per diem rate used
h. Total per diem charged
i. Transportation costs (rental car, air fare, etc.)
j. Total charges
k. Explanation of variances exceeding 10% of the approved versus actual costs
l. Indirect handling rate

6.3.2 NON-GSA FEDSIM-ISSUED ORDER INVOICE REQUIREMENTS

For non-GSA FEDSIM-issued Orders, the contractor shall follow specific invoice requirements for CLIN type (FFP or LH), and travel, as indicated in the order.

6.4 INVOICE SUBMISSION

6.4.1 FOR GSA FEDSIM-ISSUED ORDERS

The BPA team lead shall submit Requests for Payments in accordance with the format contained in General Services Administration Acquisition Manual (GSAM) 552.232-25, PROMPT PAYMENT (NOV 2009), to be considered proper for payment. In addition, the following data elements shall be included on each invoice.

Order Number: *(from GSA Form 300, Block 2)*
Paying Number: *(ACT/DAC NO.) (From GSA Form 300, Block 4)*
FEDSIM Project Number: (Fill in project number)
Project Title: (Fill in project title)

The contractor shall certify with a signed and dated statement that the invoice is correct and proper for payment.

The contractor shall provide invoice backup data in accordance with the contract type, including detail such as labor categories, rates, and quantities of labor hours per labor category.

The contractor shall submit invoices as follows:

The contractor shall utilize FEDSIM's electronic Tracking and Ordering System (TOS) to submit invoices. The contractor shall submit invoices electronically by logging onto the following link (requires Internet Explorer to access the link):

https://portal.fas.gsa.gov

Select *Vendor Support*, log in using your assigned I.D. and password, then click on *Create Invoice*. The TOS Help Desk should be contacted for support at 877-472-4877 (toll free). By utilizing this method, no paper copy of the invoice shall be submitted to GSA FEDSIM or the GSA Finance Center. However, the FEDSIM COR may require the contractor to submit a written "hardcopy" invoice with the client's certification prior to invoice payment.

6.4.2 FOR NON-GSA FEDSIM-ISSUED ORDERS

The contractor shall follow the specific invoice requirements indicated in the order.

6.5 ACQUISITION, CONTRACTING, AND TECHNICAL FEE

As stated in Section 1.5.1, the contractor shall send the ACT fee to the address below. Please note the ACT fee does not apply to orders issued by GSA or DHS.

The contractor shall provide a copy of the BPA CO/COR approved Report of Sales (Section 9, Attachment M) for the appropriate period, to accompany the remittance of the ACT Fees to enable verification of the fee amounts rendered.

ACT Fees shall be sent to:

Payments should be sent via USPS to:

USDA c/o GSA
PO Box 979009
St. Louis, MO 63197-9009

If the payments are sent via FedEx or UPS, please send to:

USDA c/o GSA
Lockbox 979009
1005 Convention Plaza
St. Louis, MO 63101
SL-MO-C2GL

7.1 KEY PERSONNEL

Individual orders may designate, or require the contractor to propose, a minimum number of personnel who shall be designated as "Key." Additionally, the contractor may propose Key Personnel based on the needs of their quoted solution. Unless otherwise stated in the order, the Government desires that Key Personnel be assigned for the duration of the order. Key Personnel may be replaced or removed subject to Section 7.1.1 - Special Contract Requirements, Key Personnel Substitution.

7.1.1 KEY PERSONNEL SUBSTITUTION

The contractor shall not replace any personnel designated as Key Personnel without the written concurrence of the Ordering CO. Prior to utilizing other than personnel specified in quotes in response to an RFQ, the contractor shall notify the Government Ordering CO and the Ordering COR. This notification shall be no later than ten calendar days (unless otherwise stated in the order) in advance of any proposed substitution and shall include justification (including résumé(s) and labor category of proposed substitution(s)) in sufficient detail to permit evaluation of the impact on order performance.

Substitute personnel qualifications shall be equal to, or greater than, those of the personnel being substituted. If the Government Ordering CO and the Ordering COR determine that a proposed substitute personnel is unacceptable, or that the reduction of effort would be so substantial as to impair the successful performance of the work under the order, the contractor may be subject to default action as prescribed by FAR 52.249-6 Termination (Cost Reimbursement), Alternate IV or FAR 52.249-8, Default (Fixed-Price Supply and Service).

7.1.2 BPA PROGRAM MANAGER

The contractor shall designate as Key Personnel, a BPA Program Manager (BPA PM) to serve as the Government's primary point of contact for all contractor work under this BPA. The BPA PM shall be an employee of the prime or lead contractor. The BPA PM shall be readily available to respond to Government questions, concerns, and comments, as well as be proactive in alerting the Government to potential contractual or programmatic issues. Additional functions would include customer service, program management reviews when requested by the Government, invoicing, completing the quarterly Report of Sales (see Section 1.5.1), payment of the ACT fee, and submission of any reports required by the BPA CO. The Government expects the cost for the BPA Program Manager to be captured as overhead. Orders issued under this BPA may not include labor categories for and/or invoice for the BPA Program Manager.

BPA Program Manager: (b) (6)

7.1.2.1 PROGRAM MANAGEMENT REVIEW (PMR)

The contractor shall conduct a PMR to be held on a United States Government fiscal year (FY), quarterly basis (e.g., October-December, January-March, April-June, July-September) at a location approved by the Government. PMR's shall include the FEDSIM CO, COR, TPOC, DHS client representatives, and additional Government and contractor representatives deemed necessary by the FEDSIM COR and/or DHS TPOC. The contractor shall work with the BPA COR to schedule the PMR. The PMR will provide a forum for Government review of progress, planning, discussion of emerging technology and issues related to the BPA. The first PMR shall occur in Q4 of FY 14 (July 2014).

7.2 GOVERNMENT-FURNISHED PROPERTY (GFP) AND GOVERNMENT FURNISHED INFORMATION (GFI)

Ordering activities using this BPA may provide the contractor with some of the necessary information, and/or office space required to perform the services outlined in the order. The contractor shall ensure that appropriate administrative, technical, and physical safeguards are established to ensure the security and confidentiality of this information, data, and/or equipment is properly protected. The contractor shall be responsible for properly protecting all information used, gathered, or developed as a result of work under the order.

In addition, the contractor shall protect all Government data, etc., by treating the information as sensitive. Sensitive but unclassified information, data, and/or equipment will only be disclosed to authorized-personnel as described in the order. The contractor shall keep the information confidential, use appropriate safeguards to maintain its security in accordance with minimum Federal standards.

When no longer required, this information, data, and/or equipment shall be returned to Government control, destroyed, or held until otherwise directed by the Ordering CO. The contractor shall destroy unneeded items by burning, shredding, or any other method that precludes the reconstruction of the material.

Work under specific orders may require that the contractor's personnel to have access to Privacy Information. Contractor personnel shall adhere to the Privacy Act, Title 5 of the U.S. Code, section 552a and applicable agency rules and regulations.

7.3 ACCESS TO FACILITIES, SYSTEMS AND SECURITY CLEARANCE REQUIREMENTS

The ordering activity, or agencies being supported by orders under this BPA, may have specific personnel security and background check requirements in order for contractor personnel to access the facilities and systems necessary to perform the work. When these requirements exist, they will be detailed in the RFQ, along with any special instructions.

Individual orders under this BPA may also require work be performed up to the Top Secret / Sensitive Compartmented Information (TS/SCI) level, and/or in Government facilities that require personnel to have TS/SCI clearances in order to enter the facility.

7.4 SECURITY REQUIREMENTS

This section provides the minimum requirements for a CDM Tools and CMaaS Offering. The contractor is responsible for providing, securing, monitoring, and maintaining the hardware, network(s), and software that support the infrastructure and present the CDM tools and services to the ordering activity.

The implementation of a new Federal Government IT system requires a formal approval process known as Assessment and Authorization with continuous monitoring. The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37, Revision 1, "Guide for applying the Risk Management Framework to Federal Information System," (hereafter described as NIST 800-37) gives guidelines for performing the Assessment and Authorization (A&A) process. In addition, NIST SP 800-53 provides guidance regarding appropriate controls for each system.

An independent third-party assessment may be required by orders under this BPA of the contractor's security controls to determine the extent to which security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting security requirements. The ordering activity's security assessment staff will be available for consultation during the process, and will review the results before issuing an Assessment and subsequent Authorization decision. The Government reserves the right to verify the infrastructure and security test results before issuing an Authorization decision.

The contractor is advised to review the NIST documents to determine the level of effort that will be necessary to complete the requirements.

Ordering activities, including non-Federal entities, such as state governments, may have other security provisions defined at the order level.

7.4.1 ORDERING ACTIVITY SYSTEM SECURITY COMPLIANCE REQUIREMENT

The data that will be processed by the information systems being requested by ordering activities in support of specific order requirements will be classified by the respective agencies' Office of the Chief Information Officer (OCIO), or equivalent if no OCIO, for impact in the RFQ, in all three categories (confidentiality, integrity, and availability) as defined in Federal Information Processing Standards (FIPS) Pub 199, "Standards for Security Categorization of Federal Information and Information Systems." The three categories are defined as follows:

Definitions:

a. CONFIDENTIALITY: "Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…" [44 U.S.C, Sec 3542] A loss of confidentiality is the unauthorized disclosure of information.

b. INTEGRITY: "Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity…" [44 U.S.C., Sec 3542] A loss of integrity is the unauthorized modification or destruction of information.

c. AVAILABILITY: "Ensuring timely and reliable access to and use of information…" [44 U.S.C., Sec 3542] A loss of availability is the disruption of access to or use of information or an information system.

NIST Special Publication 800-53 Revision 3, "Recommended Security Controls for Federal Information Systems" (hereafter described as NIST SP 800-53) defines requirements for compliance to meet the minimum security requirements. NIST SP 800-53 requirements are viewed as mandatory requirements for which some risks are acceptable, but generally most requirements pertaining to the impact level must be incorporated into the infrastructure. The controls requiring organizational defined parameter will be provided by the ordering activity within the individual RFQ.

The contractor shall implement the controls from NIST SP 800-53 for the appropriate impact level (as defined in FIPS 199). The Government has determined that the appropriate impact level for CDM systems is "high" for confidentiality and integrity and "moderate" for availability.

The contractor shall generally and substantially and in good faith follow NIST guidelines and any security guidance provided by the ordering activity, or activity being supported by the order, as appropriate. Where there are no procedural guides, the contractor shall use generally accepted industry best practices for IT security.

7.4.2 REQUIRED SECURITY POLICIES AND REGULATIONS

To perform work on orders under this BPA, the contractor shall be subject to all ordering activity IT security standards, policies, reporting requirements, and Government-wide laws or regulations applicable to the protection of Government-wide information security.

Contractors are also required to comply with FIPS, the "Special Publications 800 series" guidelines published by NIST, and the requirements of FISMA.

a. Federal Information Security Management Act (FISMA) of 2002.
b. Clinger-Cohen Act of 1996 also known as the "Information Technology Management Reform Act of 1996."
c. Privacy Act of 1974 (5 U.S.C. § 552a).
d. Homeland Security Presidential Directive (HSPD-12), "Policy for a Common Identification Standard for Federal Employees and Quoters," August 27, 2004.
e. Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources," and Appendix III, "Security of Federal Automated Information Systems," as amended.
f. OMB Memorandum M-04-04, "E-Authentication Guidance for Federal Agencies."
g. FIPS PUB 199, "Standards for Security Categorization of Federal Information and Information Systems."
h. FIPS PUB 200, "Minimum Security Requirements for Federal Information and Information Systems."
i. FIPS PUB 140-2, "Security Requirements for Cryptographic Modules."
j. NIST Special Publication 800-18 Rev 1, "Guide for Developing Security Plans for Federal Information Systems."
k. NIST Special Publication 800-30, "Risk Management Guide for Information Technology Security Risk Assessment Procedures for Information Technology Systems."
l. NIST Special Publication 800-34, "Contingency Planning Guide for Information Technology Systems."

m. NIST SP 800-37, Revision 1, "Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach."
n. NIST Special Publication 800-47, "Security Guide for Interconnecting Information Technology Systems."
o. NIST Special Publication 800-53 Revision 4, "Recommended Security Controls for Federal Information Systems."
p. NIST Special Publication 800-53A, "Guide for Assessing the Security Controls in Federal Information Systems."

7.4.2.1 SUPPLY CHAIN RISK MANAGEMENT / COMPANY INFORMATION REVIEW

The security of the US Government's supply chain in cybersecurity acquisitions is a growing and evolving risk. A supply chain element of great concern is control or ownership of a company (or component of a company) by a foreign entity that has the ability to, directly or indirectly, influence or outright control the appointment/election of key leadership personnel (such as officers, directors, board members, etc.), and decisions affecting company operations and investments that could pose a supply chain risk. Continuously reviewing and assessing these relationships and their impacts on the cybersecurity supply chain is key to protecting the government's enterprise system investments that the CDM program aims to defend and strengthen through continuous monitoring.

The contractor shall support supply chain protections as defined in the NIST 800-53 SA-12 control. The NIST 800-53 SA-12 control requires organizations to protect supply chains as follows: "The organization protects against supply chain threats to the information system, system component, or information system service by employing (Assignment: organization-defined security safeguards) as part of a comprehensive, defense-in-breadth information security strategy." NIST 800-53 SA-12 can be located at the NIST website; http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

For purposes of supply chain risk assessment under this BPA, the "organization-defined security safeguards" referenced above include a Company Information Review (CIR) that will be conducted by DHS during each delivery order or task order award, if specified in the RFQ. The contractor shall submit a completed Acquisition Risk Questionnaire (ARQ) **(see Section 9 – Attachment S)** with quote submissions under this BPA in accordance with the delivery order or task order RFQ instructions to supplement the CIR. ARQ responses must reference the parent company and all subsidiary entities. Additionally, the contractor will be required to request, collect, and submit an ARQ for all proposed CTA members and all tiers of subcontractors performing services or supplying products with delivery/task order quote submissions. The Contracting Officer shall consider any negative CIR findings (as determined by DHS) in determining if the contractor or any proposed CTA member or subcontractor presents an undue supply chain risk to the task order award as part of the Contracting Officer's pre-award responsibility determination on the apparent awardee of the Delivery Order/Task Order.

7.4.3 ASSESSMENT AND AUTHORIZATION (A&A) ACTIVITIES

For orders under this BPA that require the contractor to implement a new Federal Government IT system, this new system requires a formal approval process known as Assessment and Authorization (A&A) process. NIST Special Publication 800-37 gives guidelines for performing the A&A process. The impact level and A&A needs for specific requirements will be defined by the specific RFQ. The failure to obtain and maintain a valid authorization will be grounds for cancellation of the award and termination of any outstanding orders. Any contractor-supplied software or hardware will be subject to the same monitoring as any other system on the agency's IT infrastructure.

Authorization is required by each customer agency before the system is deemed operational and/or connected to the agency's network, consistent with existing law and regulations. It is expected that one Federal-level assessment will be largely an adequate basis for risk assessment and authorization for most agencies, but that each agency may required specific additional assessment items to be specified in orders.

7.4.3.1 ASSESSMENT OF SYSTEM

For orders under this BPA, the contractor shall comply with NIST Special Publication 800-37 requirements as mandated by Federal laws and policies, including making available any documentation, physical access, and logical access needed to support this requirement. The Level of Effort for the A&A is based on the System's NIST FIPS Publication 199 categorization (see Section 7.4.1). The contractor shall create, maintain, and update the following A&A documentation:

a. System Security Plan (SSP) completed in agreement with NIST Special Publication 800-18, Revision 1. The SSP shall include as appendices required policies and procedures across 18 control families mandated per FIPS 200, Rules of Behavior, and Interconnection Agreements (in agreement with NIST Special Publication 800-47).
b. Contingency Plan (including Disaster Recovery Plan) completed in agreement with NIST Special Publication 800-34.
c. Contingency Plan Test Report completed in agreement with GSA IT Security Procedural Guide 06-29, "Contingency Plan Testing."
d. Plan of Actions & Milestones completed in agreement with GSA IT Security Procedural Guide 09-44, "Plan of Action and Milestones (POA&M) and/or based on the continuous monitoring data of the CDM system.
e. Independent Penetration Test Report documenting the results of vulnerability analysis and exploitability of identified vulnerabilities.

Information systems must be assessed whenever there is a significant change to the system's security posture in accordance with NIST Special Publication 800-37 Revision 1, "Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach."

At the High impact level, the contractor shall be responsible for providing an independent Security Assessment/Risk Assessment in accordance with NIST Special Publication 800-37 Revision 1, "Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach."

The Government reserves the right to perform Penetration Testing. If the Government exercises this right, the contractor shall allow Government employees (or designated third-party auditors) to conduct Assessment and Authorization (A&A) activities to include control reviews in accordance with NIST 800-53/NIST 800-53A. Review activities include, but are not limited to, operating system vulnerability scanning, web application scanning, and database scanning of applicable systems that support the processing, transportation, storage, or security of Government information. This includes the general support system infrastructure.

Identified gaps between required 800-53 controls and the quote's implementation as documented in the Security Assessment/Risk Assessment report shall be tracked for mitigation in a Plan of Action and Milestones (POA&M) document. Depending on the severity of the gaps, the Government may require them to be remediated before an Authorization to Operate is issued.

The contractor is responsible for mitigating all security risks found during A&A and continuous monitoring activities. All high-risk vulnerabilities must be mitigated within 30 calendar days and all moderate risk vulnerabilities must be mitigated within 90 calendar days from the date vulnerabilities are formally identified. The Government will determine the risk rating of vulnerabilities.

7.4.3.2 AUTHORIZATION OF SYSTEM

For orders under this BPA that require A&A, the process to authorize the system follows. Upon receipt of the documentation described in the NIST Special Publication 800-37 and as documented above, the appropriate Authorizing Officials (AOs) for the system (in coordination with the ordering activity Senior Agency Information Security Officer (SAISO), system Program Manager, Information System Security Manager (ISSM), and Information System Security Officer (ISSO)) will render an Authorization decision to:

a. Authorize system operation w/out any restrictions or limitations on it operation,
b. Authorize system operation w/ restriction or limitation on its operation, or
c. Not authorize for operation.

The contractor shall provide access to the Federal Government, or their designee acting as their agent, when requested, in order to verify compliance with the requirements for an Information Technology security program. The Government reserves the right to conduct on-site inspections. The contractor shall make appropriate personnel available for interviews and documentation during this review. If documentation is considered proprietary or sensitive, these documents may be reviewed on-site under the hosting contractor's supervision.

7.4.4 REPORTING AND CONTINUOUS MONITORING

For systems the contractor has provided through orders under this BPA, maintenance of the security Authorization to Operate will be through continuous monitoring and periodic audit of the operational controls within a contractor's system, environment, and processes to determine if the security controls are meeting Government regulatory and compliance requirements. Through continuous monitoring, security controls and supporting deliverables Authority to Operate will be maintained and submitted to an ordering activity in accordance with customer IT security standards, policies, and reporting requirements.

NIST published SP800-86 Guide to Integrating Forensic Techniques into Incident Response. SP800-86 defines in a much more precise and specific way the procedures, issues and technologies required to move an incident from the point of discovery all the way through to resolution.

7.4.5 ADDITIONAL SECURITY STIPULATIONS

If required by a specific order under this BPA, deliverables designated in the RFQ shall be labeled "FOR OFFICIAL USE ONLY" (FOUO) or contractor selected designation per document sensitivity. External transmission/dissemination of FOUO to or from a Government computer must be encrypted. Certified encryption modules must be used in accordance with FIPS PUB 140-2, "Security requirements for Cryptographic Modules."

Any classification of the data collected shall be determined by the classification guide of each agency where the system is deployed. Should data be deemed classified, additional appropriate security requirements shall be specified in the order.

As prescribed in the Federal Acquisition Regulation (FAR) 24.104, if the system involves the design, development, or operation of a system of records on individuals, the contractor shall implement requirements in FAR clause 52.224-1, "Privacy Act Notification" and FAR clause 52.224-2, "Privacy Act."

The Government has the right to perform manual or automated audits, scans, reviews, or other inspections of the vendor's IT environment being used to provide or facilitate services for the Government. The contractor shall be responsible for privacy and security safeguard provisions in accordance with FAR clause 52.239-1 "Privacy and Security Safeguards."

The contractor shall not publish or disclose in any manner, including responding to press inquiries, without the Ordering CO's written consent, the details of any security safeguards either designed or developed by the contractor in support of an order under this BPA, or otherwise provided by the Government.

To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of any non-public Government data collected and stored by the contractor, the contractor shall afford the Government logical and physical access to the contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases within 72 hours of the request. Automated audits shall include, but are not limited to, the following methods:

a. Authenticated and unauthenticated operating system/network vulnerability scans.
b. Authenticated and unauthenticated web application vulnerability scans.
c. Authenticated and unauthenticated database application vulnerability scans.

Automated scans may be performed by Government personnel, or agents acting on behalf of the Government, using Government-operated equipment, and Government-specified tools. If the contractor chooses to run its own automated scans or audits, results from these scans may, at the Government's discretion, be accepted in lieu of Government performed vulnerability scans. In these cases, scanning tools and their configuration shall be approved by the Government. In addition, the results of vendor-conducted scans shall be provided, in full, to the Government.

If new or unanticipated threats or hazards are discovered by either the Government or the contractor, or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attention of the other party.

7.5 ORGANIZATIONAL CONFLICT OF INTEREST AND NON-DISCLOSURE REQUIREMENTS

7.5.1 ORGANIZATIONAL CONFLICT OF INTEREST

For work to be performed in support of a specific order under this BPA, if the contractor has or is currently providing support or anticipates providing support to the department or agency, for whom order work is being performed, that creates or represents an actual or potential organizational conflict of interest (OCI), the contractor shall immediately disclose this actual or potential OCI in accordance with FAR Subpart 9.5. For each order, the contractor is also required to complete and sign an Organizational Conflict of Interest Statement in which the contractor (and any subcontractors, consultants or teaming partners) agrees to disclose information concerning the actual or potential conflict with any quote for any solicitation relating to any work in the order. All actual or potential OCI situations shall be handled in accordance with FAR Subpart 9.5.

7.5.2 NON-DISCLOSURE REQUIREMENTS

If the contractor acts on behalf of, or provides advice with respect to any phase of an agency procurement, as defined in FAR 3.104-4, then the contractor shall ensure that all its personnel (to include subcontractors, teaming partners, and consultants) who will be personally and substantially involved in the performance of the order:

a. Execute and submit a Corporate Non-Disclosure Agreement (NDA), using procedures outlined in the order RFQ, prior to the commencement of any work on the order, and
b. Are instructed in the FAR 3.104 requirements for disclosure, protection, and marking of contractor bid or quote information, or source selection information.

All proposed replacement contractor personnel also must submit a Non-Disclosure Agreement and be instructed in the requirements of FAR 3.104. Any information provided by contractors in the performance of order work under this BPA, or obtained by the Government, is only to be used in the performance of the order. The contractor shall put in place appropriate procedures for the protection of such information and shall be liable to the Government for any misuse or unauthorized disclosure of such information by its personnel, as defined above.

7.6 SECTION 508 COMPLIANCE REQUIREMENTS

Unless the Government invokes an exemption for work performed in support of individual orders under this BPA, all Electronic and Information Technology (EIT) products and services proposed shall comply with Section 508 of the Rehabilitation Act of 1973, per the 1998 Amendments, 29 United States Code (U.S.C.) 794d, and the Architectural and Transportation Barriers Compliance Board's Electronic and Information Technology Accessibility Standards at 36 Code of Federal Regulations (CFR) 1194, as required by contractor's Schedule 70 contract. If required at the order level, the contractor shall identify all EIT products and services proposed, identify the technical standards applicable to all products and services proposed, and state the

degree of compliance with the applicable standards. Additionally, the contractor must clearly indicate where the information pertaining to Section 508 compliance can be found (e.g., Vendor's or other exact web page location). The contractor must ensure that this information pertaining to 508 compliance is easily accessible beginning at time of award.

Specific order RFQs may require Section 508 compliance testing or verification to be performed prior to order award, or prior to acceptance of deliverables.

7.7 TRAVEL

7.7.1 TRAVEL REGULATIONS

Contractor costs for travel will be reimbursed at the limits set in the following regulations (see FAR 31.205-46):

a. Federal Travel Regulations (FTR) - prescribed by the GSA, for travel in the contiguous U.S.
b. Joint Travel Regulations (JTR), Volume 2, Department of Defense (DoD) Civilian Personnel, Appendix A - prescribed by the DoD, for travel in Alaska, Hawaii, and outlying areas of the U.S.
c. Department of State Standardized Regulations (DSSR) (Government Civilians, Foreign Areas), Section 925, "Maximum Travel Per Diem Allowances for Foreign Areas" - prescribed by the Department of State, for travel in areas not covered in the FTR or JTR.
d. Any other specific regulations detailed at the individual order level.

7.7.2 TRAVEL AUTHORIZATION REQUESTS

Before undertaking travel to any Government site or any other site in performance of order work under this BPA, the contractor shall have this travel approved by, and coordinated with, the order CO or order COR using procedures detailed in the specific order RFQ.

7.8 COMMERCIAL SOFTWARE AGREEMENTS

The Government understands that commercial software tools will be purchased in furtherance of this BPA and subsequent orders as described in Section 2 – Description / Specification / Statement of Work, Section 7.8 and Section 1.2, and may be subject to commercial agreements which may take a variety of forms, including without limitation, licensing agreements, terms of service, maintenance agreements, and the like, whether existing, in hard copy or in an electronic or online format such as "clickwrap" or "browsewrap" (collectively, "Software Agreements"). The parties acknowledge that the FAR clause at 12.212(a) requires the Government to procure such tools and their associated documentation under such Software Agreements to the extent such Software Agreements are consistent with Federal law and Government needs.

7.8.1 CONSISTENCY WITH FEDERAL LAW

In order to ensure that the Software Agreements are consistent with Federal law, the contractor shall not make any purchase contemplated in Section 7.8, or quote software to meet the requirements of Section 2, without first securing the consent of the licensor of such software tools to amend the Software Agreements in accordance with the Amendment clause set forth in

Section 7.8.2. The contractor shall submit documentary evidence of such consent as part of its technical proposal.

7.8.2 AMENDMENT OF COMMERCIAL SOFTWARE AGREEMENTS

The requirements of this Section 7.8 apply only to those commercial software tools newly purchased under this BPA and subsequent orders; they do not apply to software furnished as GFI/GFE (if any). Further, they apply only to those Software Agreements that define the Government as the licensee, or are intended to be transferred or assigned to the Government, with the Government becoming the licensee, at the end of an order under this BPA.

The following is the amendment clause. As used in the Amendment clause, the term "this Agreement" refers to each Software Agreement. The relevant definitions and the capitalization of terms (e.g., Licensee, Licensor, Software, Agreement) may be adjusted as necessary to match the nomenclature of the Software Agreement.

Amendment

For Federal Government Licensees, this Agreement is hereby amended as follows:

1. ***Dispute resolution and governing law:*** Any arbitration, mediation, or similar dispute resolution provision in this Agreement is hereby deleted. This Agreement shall be governed by and interpreted and enforced in accordance with the laws of the United States of America, and dispute resolution shall take place in a forum, and within the time period, prescribed by applicable federal law. To the extent permitted by Federal law and then only to the extent not pre-empted by Federal law, the laws of the state specified in this Agreement (excluding its choice of law rules) will apply. No equitable or injunctive relief, and no shifting of legal fees or costs, may be sought against the Federal Government Licensee except as, and then only to the extent, specifically authorized by applicable Federal statute.

2. ***Indemnification***: Any provisions in this Agreement requiring any Federal Government Licensee to indemnify any party are hereby deleted and shall not apply. Any provisions requiring the licensor to indemnify the Federal Government Licensee shall be revised to state that such indemnification, and the conduct and/or settlement of any applicable proceedings, shall be subject to 28 USC 516.

3. ***Changes in templates***: This Agreement shall apply in the version attached hereto. Subsequent updates to or changes in the licensor's standard commercial templates for such agreements shall not be binding on the Federal Government Licensee, except by prior express written agreement of both parties.

4. ***Fees, taxes, and payment:*** If the software is licensed as part of a separate Government contract between the Federal Government Licensee and a prime contractor, the provisions of such contract regarding fees, taxes and payment

shall supersede any provisions of this Agreement regarding same. Notwithstanding the foregoing: (a) express written agreement of the Federal Government Licensee shall be required prior to (i) any extension or renewal of this Agreement or the associated fees or (ii) any change in the fees; (b) late payments shall be governed by the Prompt Payment Act and the regulations at 5 CFR 1315; and (c) no cost of collection on delinquent invoices may be sought against the Federal Government Licensee except as, and then only to the extent, specifically authorized by applicable federal statute.

5. ***Assignment*:** Licensor may not assign this Agreement or its rights or obligations there under, in whole or in part, except in accordance with the procedures set forth in FAR subparts 32.8 and/or 42.12, as applicable.

6. ***No waiver of liability or cause of action***: Any provision requiring the Federal Government Licensee to agree to waive or otherwise not to pursue any claim against the licensor it may otherwise have is hereby deleted. Without limiting the generality of the foregoing, the parties agree that nothing in this Agreement, including but not limited to the limitation of liability clauses, in any way grants the licensor a waiver from, release of, or limitation of liability pertaining to, any past, current or future violation of federal law and that no clause restricting users' statements shall be read to restrict the Federal Government Licensee's ability to pursue any course of action otherwise permitted by federal law, regulation, or policy, including without limitation making public statements in connection with any suspension or debarment action.

7. ***Audit***: Any clauses in this Agreement allowing for an audit of the Federal Government Licensee's records or information systems, or verification of its compliance with this Agreement generally, shall be subject to the Federal Government Licensee's requirements pertaining to security matters, including without limitation clearances to be held and non-disclosure agreements to be executed by auditors, badging or escorting requirements for access to premises, and other applicable requirements. Any over-use identified in an audit shall be referred to the prime contractor or the Federal Government Licensee's contracting officer (as applicable) for action. No audit costs may be sought against the Federal Government Licensee except as, and then only to the extent, specifically authorized by applicable federal statute.

8. ***Compliance with laws*:** The parties acknowledge that the United States, as a sovereign, is subject to the laws of the United States. Nothing in this Agreement shall be interpreted to imply consent by any Federal Government Licensee to submit to the adjudicative or enforcement power of any regulatory, administrative, or judicial authority of, or the application of the laws of, another jurisdiction. Any provision inconsistent with applicable federal law that is not listed above is hereby deemed omitted from this Agreement to the extent of such inconsistence.

9. ***Third party terms***: Any third-party licensing terms associated with third-party software components or products embedded in or otherwise provided with the Software shall be deemed amended in accordance with Sections 1-8 above.

7.9 CONTRACTOR IDENTIFICATION

If the ordering activity is a DoD activity, or the work being performed in support of a specific order under this BPA requires that contractor personnel enter DoD facilities, or interact with DoD personnel, as stated in 48 CFR 211.106, Purchase Descriptions for Service Contracts, contractor personnel shall identify themselves as contractor personnel by introducing themselves or being introduced as contractor personnel and by displaying distinguishing badges or other visible identification for meetings with Government personnel. Contractor personnel shall appropriately identify themselves as contractor employees in telephone conversations and in formal and informal written correspondence.

7.10 INTELLECTUAL PROPERTY RIGHTS

The existence of any patent, patent application or other intellectual property right that encumbers any deliverable must be disclosed in writing on the cover letter that accompanies the delivery. If no such disclosures are provided, the data rights provisions in FAR 52.227-14, Rights in Data – General, Alt. II and III apply. The Software Agreements referenced in Section 7.8, amended as contemplated therein, shall be deemed to constitute such disclosure with regard to their associated commercial software tools and shall prevail over any inconsistent provision in FAR 52.227-14, Rights in Data – General, Alt. II and III to the extent of such inconsistency.

7.11 FEDERAL DESKTOP CORE-CONFIGURATION (FDCC) & U.S. GOVERNMENT CONFIGURATION BASELINE (USGCB)

The contractor shall certify that when applicable, software applications and tools are fully functional and operate correctly as intended on systems using the FDCC and/or USGCB as appropriate (see the National Institute of Standards and Technology [NIST] websites: http://usgcb.nist.gov/index.html and http://nvd.nist.gov/fdcc/index.cfm). This requirement only applies for software products and tools that are intended to run on operating systems covered by FDCC and USGCB. The standard installation, operation, maintenance, updates, and/or patching of software shall not alter the configuration settings from the approved FDCC/USGCB configuration. For offerings that require installation, the information technology should follow OMB memorandum 07-18. Applications designed for normal end users shall run in the standard user context without elevated system administration privileges. The contractor shall use Security Content Automation Protocol (SCAP) validated tools with FDCC/USGCB Scanner capability to certify their products operate correctly with FDCC/USGCB configurations and do not alter FDCC/USGCB settings.

7.12 COMPLIANCE WITH INTERNET PROTOCOL VERSION 6 (IPv6) IN ACQUIRING INFORMATION TECHNOLOGY

This contract involves the acquisition of IT that uses Internet Protocol (IP) technology. The contractor agrees that (1) all deliverables that involve IT that uses IP (products, services, software, etc.) comply with IPv6 standards and interoperate with both IPv6 and IPv4 systems and

products; and (2) it has IPv6 technical support for fielded product management, development and implementation available. If the contractor plans to offer a deliverable that involves IT that is not initially compliant, the contractor agrees to (1) obtain the Contracting Officer's approval before starting work on the deliverable; and (2) have IPv6 technical support for fielded product management, development and implementation available.

Full technical specifications for Hosts, Routers, and Network Protection products recommend by NIST for acquisition in the Federal Government can be found in NIST SP 500-267 USGv6 profile.

Should the contractor find that the Statement of Work or specifications of this contract do not conform to IPv6 standards; it must notify the Contracting Officer of such nonconformance and act in accordance with the instructions of the Contracting Officer.

7.13 SUBSTITUTION AND TECHNOLOGY REFRESH

If at any time during the life of this BPA, the original manufacturer of the equipment (includes software, hardware, and firmware) schedules the products for discontinuation, improvement and/or replacement, within seven (7) days of the BPA holder's awareness of the Original Equipment Manufacturers' (OEM) intent, the BPA holder shall request a modification to their BPA using Attachment Q – Template for Modifications to include the revised products on the BPA. Improvement of product includes new releases, updates, and upgrades including additional features and functionality and successor products. Contractors shall not quote replacement products for addition to the BPA unless those products are already available on the contractor's GSA Schedule contract. Quoted prices for replacement products shall be in accordance with the offeror's GSA Schedule pricing for that product. Discounts shall be at the same or greater discount level as the original BPA product price. The request for modification shall be submitted to the BPA CO/CS and COR, in order for replacement products to be formally added by the BPA CO via modification to the BPA.

7.14 NEW PRODUCTS

Within a month of the BPA holder's quarterly PMR, a contractor can request a new product or products be added to their BPA. The new product(s) can be added via a request for modification submitted to the BPA CO/CS and COR. The contractor shall submit their request for modification by using Attachment Q – Template for modifications and Attachment R – BPA Requirements Checklist Product Adds, indicating only those products they wish to add. Contractors shall not quote products for addition to the BPA unless those products are already available on the contractor's GSA Schedule contract. All new products requested to be added to the BPA must be formally approved via modification by the BPA CO.

7.15 CONTRACTING TEAMING AGREEMENT (CTA) MEMBERS AND SUBCONTRACTORS

At the BPA level, a contractor can request a new CTA to be added or removed to/from their BPA within a month of the BPA holders quarterly PMR. This request should occur at the same time as the request for new product adds. The Government may allow the offeror to add a CTA member if the CO determines the addition to be in the best interest of the Government. The process to add a new CTA is via a request for modification submitted to the BPA CO/CS and COR. The request for modification shall include a copy of each teaming partner's applicable GSA Schedule contract to substantiate the rates offered and that the products and services are on Schedule. In addition, a copy of each applicable CTA agreement shall be submitted.

Subcontractors may be added or removed, at any time, during the BPA period of performance. The contractor shall notify the CO/CS and COR, in writing, of any such changes. An addition or removal of a subcontractor does not require a modification to the BPA. If a subcontractor is added, all labor and materials proposed must be contained within and their prices must be in accordance with the prime contractor's GSA Schedule Contract.

7.16 ECONOMIC PRICE ADJUSTMENTS (EPA)

If at any time during the life of the BPA, a product/service that is included on the BPA holder's awarded Attachment K or Attachment L undergoes an EPA modification at the Schedule 70 level, the BPA holder shall notify the Government and submit a BPA modification request within seven (7) days of the BPA holder's awareness of that adjustment. BPA holders shall utilize Attachment Q- Template for Modifications to submit the revised pricing for the products/services on the BPA that were adjusted due to an EPA Modification at the Schedule 70 Level. Contractors shall not quote adjusted prices for products or services that are not currently on their awarded Attachment K or Attachment L. Quoted prices submitted shall be in accordance with the contractor's Schedule 70 awarded prices. Discounts shall be at the same or greater discount level as the original BPA product price. The request for modification shall be submitted to the BPA CO/CS, and the COR for formal incorporation into the BPA.

8.1 52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 1998)

This BPA incorporates one or more clauses by reference with the same force and effect as if they were given in full text. Upon request the BPA CO will make their full text available. Also, the full text of a provision may be accessed electronically at:

FAR website: https://www.acquisition.gov/far/

Clause No	Clause Title	Date
52.204-2	Security Requirements	(Aug 1996)
52.217-8	Option to Extend Services Fill-In Date: 30 days, 60 days, 5 years	(Nov 1999)
52.217-9	Option to Extend the Term of the Contract Fill-In Date: 30 days	(Mar 2000)
52.219-8	Utilization of Small Business Concerns	(Jan 2011)
52.224-1	Privacy Act Notification	(Apr 1984)
52.224-2	Privacy Act	(Apr 1984)
52.227-14	Rights In Data – General, Alternate II	(Dec 2007)
52.227-14	Rights In Data – General, Alternate III	(Dec 2007)
52.227-15	Representation of Limited Rights Data and Restricted Computer Software	(Dec 2007)
52.232-17	Interest	(Oct 2010)
52.232-18	Availability of Funds	(Apr 1984)
52.239-1	Privacy or Security Safeguards	(Aug 1996)
52.249-6	Termination (Cost Reimbursement), Alternate IV	(May 2004)
52.249-8	Default (Fixed-Price Supply and Service)	(April 1984)

8.2 GENERAL SERVICES ADMINISTRATION ACQUISITION MANUAL (GSAM) CLAUSES INCORPORATED BY REFERENCE

The full text of a provision may be accessed electronically at:

GSAM website: https://www.acquisition.gov/gsam/gsam.html

Clause No	Clause Title	Date
552.232.25	Prompt Payment	(Nov 2009)

8.3 OTHER AGENCY SPECIFIC CLAUSES

Other Agency-specific clauses will be added at the order level.

9.1 LIST OF ATTACHMENTS

Attachment	Title
A	COR Appointment Letter
B	Monthly Status Report Example
C	Travel Authorization Template
D	*Placeholder*
E	*Placeholder*
F	*Placeholder*
G	*Placeholder*
H	*Placeholder*
I	Glossary and Acronym List
J	*Placeholder*
K	Tool Band Pricing
L	CMaaS Labor Category and Rate Pricing
M	Report of Sales
N	Phase 1 Tool Detailed Requirements
N-2	Phase 2 Tool Detailed Requirements
N-BOUND	Phase 3 BOUND Detailed Requirements
N-3	Phase 3 Manage Events Detailed Requirements
N-3	Phase 3 Operate Monitor and Improve
N-3	Phase 3 Design and Build in Security
O	*Placeholder*
P	*Placeholder*
Q	Template for Modifications
R	BPA Requirements Checklist_ProductAdds
S	Acquisition Risk Questionnaire

This Page Intentionally Left Blank.

CDM CMaaS Labor Categories and Rates
CDM CMaaS Labor - Base Year

Technica®

SIN	CLIN	Offeror's GSA Schedule 70 Labor Category (use CMaaS Labor Category Description at last tab of this spreadsheet as a guideline to select appropriate category)	CMaaS Labor Category	Rate Unit	CMaaS BPA Government Site Rate	CMaaS BPA Contractor Site Rate	Offeror's GSA Schedule Holder Rate (Gov. Site)	Offeror's GSA Schedule Holder Rate (Contractor Site)	% Discount CMaaS BPA / GSA Schedule 70 Rate (Gov. Site)	% Discount CMaaS BPA / GSA Schedule 70 Rate (Contractor Site)
	0006		CMaaS Labor Category	per hour						
132-51	0006AA	Project Mgr-Technical 4	Integration Services Project Manager Senior	per hour						
132-51	0006AB	Project Mgr-Technical 2	Integration Services Project Manager Junior	per hour						
132-51	0006AC	IA-Security Engineer 4	Integration Services Subject Matter Expert I*	per hour						
132-51	0006AD	IA-Security Engineer 5	Integration Services Subject Matter Expert II*	per hour						
132-51	0006AE	Corporate Consultant	Integration Services Subject Matter Expert III*	per hour						
132-51	0006AF	Subject Matter Expert 6	Integration Services System Architect	per hour						
132-51	0006AG	Computer Programmer 1	Integration Services System Programmer I*	per hour						
132-51	0006AH	Computer Programmer 2	Integration Services System Programmer II*	per hour						
132-51	0006AI	Computer Programmer 3	Integration Services System Programmer III*	per hour						
132-51	0006AJ	Systems Analyst 2	Integration Services Hardware/Software Specialist I*	per hour						
132-51	0006AK	Systems Analyst 2.5	Integration Services Hardware/Software Specialist II*	per hour						
132-51	0006AL	Systems Analyst 3	Integration Services Hardware/Software Specialist III*	per hour						
132-51	0006AM	Test Engineer 3	Integration Services Quality Assurance / Test Manager	per hour						
132-51	0006AN	Quality Assurance Specialist 1	Integration Services Quality Assurance Analyst I*	per hour						
132-51	0006AO	Quality Assurance Specialist 2	Integration Services Quality Assurance Analyst II*	per hour						
132-51	0006AP	Quality Assurance Specialist 3	Integration Services Quality Assurance Analyst III*	per hour						
132-51	0006AQ	Proces Engineer 4	Integration Services Change Management Lead	per hour						
132-51	0006AR	Proces Engineer 4 EGM	Data Integration Manager	per hour						
132-51	0006AS	Process Engineer 2	Data Integration Analyst / Specialist I*	per hour						
132-51	0006AT	Proces Engineer 3	Data Integration Analyst / Specialist II*	per hour						
132-51	0006AU	Proces Engineer 4	Data Integration Analyst / Specialist III*	per hour						
132-51	0006AV	Systems Engineer 4 EGM	Sensor Integration / Operations Manager	per hour						
132-51	0006AX	Systems Engineer 1	Sensor Integration / Operations Specialist I*	per hour						
132-51	0006AY	Systems Engineer 3	Sensor Integration / Operations Specialist II*	per hour						
132-51	0006AZ	Systems Engineer 4	Sensor Integration / Operations Specialist III*	per hour						
132-51	0006BA	Training Developer 4	Governance, Training and Policy Manager	per hour						
132-51	0006BB	Training Developer 2	Governance Training and Policy Specialist I*	per hour						
132-51	0006BC	Training Developer 2.5	Governance Training and Policy Specialist II*	per hour						
132-51	0006BD	Training Developer 3	Governance Training and Policy Specialist III*	per hour						
132-51	0006BE	IA-Security Engineer 4	Data and System Security Manager	per hour						
132-51	0006BF	IA-Security Engineer 1	Data and System Security Analyst / Specialist I	per hour						
132-51	0006BG	IA-Security Engineer 2	Data and System Security Analyst / Specialist II*	per hour						
132-51	0006BH	IA-Security Engineer 3	Data and System Security Analyst / Specialist III*	per hour						
			* for purposes of labor categories, a level "I" is the most junior, least experienced resource, while a level "III" is most senior, and most experienced.							

(b) (4)

CDM CMaaS Labor Categories and Rates
CDM CMaaS Labor - Option Year 1

Technica®

SIN	CLIN	Offeror's GSA Schedule 70 Labor Category (use CMaaS Labor Category Description at last tab of this spreadsheet as a guideline to select appropriate category)	CMaaS Labor Category	Rate Unit	CMaaS BPA Government Site Rate	CMaaS BPA Contractor Site Rate	Offeror's GSA Schedule Holder Rate (Gov. Site)	Offeror's GSA Schedule Holder Rate (Contractor Site)	% Discount CMaaS BPA / GSA Schedule 70 Rate (Gov. Site)	% Discount CMaaS BPA / GSA Schedule 70 Rate (Contractor Site)
	1006		CMaaS Labor Category	per hour						
132-51	1006AA	Project Mgr-Technical 4	Integration Services Project Manager Senior	per hour						
132-51	1006AB	Project Mgr-Technical 2	Integration Services Project Manager Junior	per hour						
132-51	1006AC	IA-Security Engineer 4	Integration Services Subject Matter Expert I*	per hour						
132-51	1006AD	IA-Security Engineer 5	Integration Services Subject Matter Expert II*	per hour						
132-51	1006AE	Corporate Consultant	Integration Services Subject Matter Expert III*	per hour						
132-51	1006AF	Subject Matter Expert 6	Integration Services System Architect	per hour						
132-51	1006AG	Computer Programmer 1	Integration Services System Programmer I*	per hour						
132-51	1006AH	Computer Programmer 2	Integration Services System Programmer II*	per hour						
132-51	1006AI	Computer Programmer 3	Integration Services System Programmer III*	per hour						
132-51	1006AJ	Systems Analyst 2	Integration Services Hardware/Software Specialist I*	per hour						
132-51	1006AK	Systems Analyst 2.5	Integration Services Hardware/Software Specialist II*	per hour						
132-51	1006AL	Systems Analyst 3	Integration Services Hardware/Software Specialist III*	per hour						
132-51	1006AM	Test Engineer 3	Integration Services Quality Assurance / Test Manager	per hour						
132-51	1006AN	Quality Assurance Specialist 1	Integration Services Quality Assurance Analyst I*	per hour						
132-51	1006AO	Quality Assurance Specialist 2	Integration Services Quality Assurance Analyst II*	per hour						
132-51	1006AP	Quality Assurance Specialist 3	Integration Services Quality Assurance Analyst III*	per hour						
132-51	1006AQ	Proces Engineer 4	Integration Services Change Management Lead	per hour						
132-51	1006AR	Proces Engineer 4 EGM	Data Integration Manager	per hour						
132-51	1006AS	Process Engineer 2	Data Integration Analyst / Specialist I*	per hour						
132-51	1006AT	Proces Engineer 3	Data Integration Analyst / Specialist II*	per hour						
132-51	1006AU	Proces Engineer 4	Data Integration Analyst / Specialist III*	per hour						
132-51	1006AV	Systems Engineer 4 EGM	Sensor Integration / Operations Manager	per hour						
132-51	1006AX	Systems Engineer 1	Sensor Integration / Operations Specialist I*	per hour						
132-51	1006AY	Systems Engineer 3	Sensor Integration / Operations Specialist II*	per hour						
132-51	1006AZ	Systems Engineer 4	Sensor Integration / Operations Specialist III*	per hour						
132-51	1006BA	Training Developer 4	Governance, Training and Policy Manager	per hour						
132-51	1006BB	Training Developer 2	Governance Training and Policy Specialist I*	per hour						
132-51	1006BC	Training Developer 2.5	Governance Training and Policy Specialist II*	per hour						
132-51	1006BD	Training Developer 3	Governance Training and Policy Specialist III*	per hour						
132-51	1006BE	IA-Security Engineer 4	Data and System Security Manager	per hour						
132-51	1006BF	IA-Security Engineer 1	Data and System Security Analyst / Specialist I	per hour						
132-51	1006BG	IA-Security Engineer 2	Data and System Security Analyst / Specialist II*	per hour						
132-51	1006BH	IA-Security Engineer 3	Data and System Security Analyst / Specialist III*	per hour						
			* for purposes of labor categories, a level "I" is the most junior, least experienced resource, while a level "III" is most senior, and most experienced.							

(b) (4)

CDM CMaaS Labor Categories and Rates
CDM CMaaS Labor - Option Year 2

Technica®

SIN	CLIN	Offeror's GSA Schedule 70 Labor Category (use CMaaS Labor Category Description at last tab of this spreadsheet as a guideline to select appropriate category)	CMaaS Labor Category	Rate Unit	CMaaS BPA Government Site Rate	CMaaS BPA Contractor Site Rate	Offeror's GSA Schedule Holder Rate (Gov. Site)	Offeror's GSA Schedule Holder Rate (Contractor Site)	% Discount CMaaS BPA / GSA Schedule 70 Rate (Gov. Site)	% Discount CMaaS BPA / GSA Schedule 70 Rate (Contractor Site)
	2006		CMaaS Labor Category	per hour						
132-51	2006AA	Project Mgr-Technical 4	Integration Services Project Manager Senior	per hour						
132-51	2006AB	Project Mgr-Technical 2	Integration Services Project Manager Junior	per hour						
132-51	2006AC	IA-Security Engineer 4	Integration Services Subject Matter Expert I*	per hour						
132-51	2006AD	IA-Security Engineer 5	Integration Services Subject Matter Expert II*	per hour						
132-51	2006AE	Corporate Consultant	Integration Services Subject Matter Expert III*	per hour						
132-51	2006AF	Subject Matter Expert 6	Integration Services System Architect	per hour						
132-51	2006AG	Computer Programmer 1	Integration Services System Programmer I*	per hour						
132-51	2006AH	Computer Programmer 2	Integration Services System Programmer II*	per hour						
132-51	2006AI	Computer Programmer 3	Integration Services System Programmer III*	per hour						
132-51	2006AJ	Systems Analyst 2	Integration Services Hardware/Software Specialist I*	per hour						
132-51	2006AK	Systems Analyst 2.5	Integration Services Hardware/Software Specialist II*	per hour						
132-51	2006AL	Systems Analyst 3	Integration Services Hardware/Software Specialist III*	per hour						
132-51	2006AM	Test Engineer 3	Integration Services Quality Assurance / Test Manager	per hour						
132-51	2006AN	Quality Assurance Specialist 1	Integration Services Quality Assurance Analyst I*	per hour						
132-51	2006AO	Quality Assurance Specialist 2	Integration Services Quality Assurance Analyst II*	per hour						
132-51	2006AP	Quality Assurance Specialist 3	Integration Services Quality Assurance Analyst III*	per hour						
132-51	2006AQ	Proces Engineer 4	Integration Services Change Management Lead	per hour						
132-51	2006AR	Proces Engineer 4 EGM	Data Integration Manager	per hour						
132-51	2006AS	Process Engineer 2	Data Integration Analyst / Specialist I*	per hour						
132-51	2006AT	Proces Engineer 3	Data Integration Analyst / Specialist II*	per hour						
132-51	2006AU	Proces Engineer 4	Data Integration Analyst / Specialist III*	per hour						
132-51	2006AV	Systems Engineer 4 EGM	Sensor Integration / Operations Manager	per hour						
132-51	2006AX	Systems Engineer 1	Sensor Integration / Operations Specialist I*	per hour						
132-51	2006AY	Systems Engineer 3	Sensor Integration / Operations Specialist II*	per hour						
132-51	2006AZ	Systems Engineer 4	Sensor Integration / Operations Specialist III*	per hour						
132-51	2006BA	Training Developer 4	Governance, Training and Policy Manager	per hour						
132-51	2006BB	Training Developer 2	Governance Training and Policy Specialist I*	per hour						
132-51	2006BC	Training Developer 2.5	Governance Training and Policy Specialist II*	per hour						
132-51	2006BD	Training Developer 3	Governance Training and Policy Specialist III*	per hour						
132-51	2006BE	IA-Security Engineer 4	Data and System Security Manager	per hour						
132-51	2006BF	IA-Security Engineer 1	Data and System Security Analyst / Specialist I	per hour						
132-51	2006BG	IA-Security Engineer 2	Data and System Security Analyst / Specialist II*	per hour						
132-51	2006BH	IA-Security Engineer 3	Data and System Security Analyst / Specialist III*	per hour						
			* for purposes of labor categories, a level "I" is the most junior, least experienced resource, while a level "III" is most senior, and most experienced.							

(b) (4)

CDM CMaaS Labor Categories and Rates
CDM CMaaS Labor - Option Year 3

Technica®

SIN	CLIN	Offeror's GSA Schedule 70 Labor Category	CMaaS Labor Category	Rate Unit	CMaaS BPA Government Site Rate	CMaaS BPA Contractor Site Rate	Offeror's GSA Schedule Holder Rate (Gov. Site)	Offeror's GSA Schedule Holder Rate (Contractor Site)	% Discount CMaaS BPA / GSA Schedule 70 Rate (Gov. Site)	% Discount CMaaS BPA / GSA Schedule 70 Rate (Contractor Site)
	3006		CMaaS Labor Category	per hour	(b) (4)					
132-51	3006AA	Project Mgr-Technical 4	Integration Services Project Manager Senior	per hour						
132-51	3006AB	Project Mgr-Technical 2	Integration Services Project Manager Junior	per hour						
132-51	3006AC	IA-Security Engineer 4	Integration Services Subject Matter Expert I*	per hour						
132-51	3006AD	IA-Security Engineer 5	Integration Services Subject Matter Expert II*	per hour						
132-51	3006AE	Corporate Consultant	Integration Services Subject Matter Expert III*	per hour						
132-51	3006AF	Subject Matter Expert 6	Integration Services System Architect	per hour						
132-51	3006AG	Computer Programmer 1	Integration Services System Programmer I*	per hour						
132-51	3006AH	Computer Programmer 2	Integration Services System Programmer II*	per hour						
132-51	3006AI	Computer Programmer 3	Integration Services System Programmer III*	per hour						
132-51	3006AJ	Systems Analyst 2	Integration Services Hardware/Software Specialist I*	per hour						
132-51	3006AK	Systems Analyst 2.5	Integration Services Hardware/Software Specialist II*	per hour						
132-51	3006AL	Systems Analyst 3	Integration Services Hardware/Software Specialist III*	per hour						
132-51	3006AM	Test Engineer 3	Integration Services Quality Assurance / Test Manager	per hour						
132-51	3006AN	Quality Assurance Specialist 1	Integration Services Quality Assurance Analyst I*	per hour						
132-51	3006AO	Quality Assurance Specialist 2	Integration Services Quality Assurance Analyst II*	per hour						
132-51	3006AP	Quality Assurance Specialist 3	Integration Services Quality Assurance Analyst III*	per hour						
132-51	3006AQ	Proces Engineer 4	Integration Services Change Management Lead	per hour						
132-51	3006AR	Proces Engineer 4 EGM	Data Integration Manager	per hour						
132-51	3006AS	Process Engineer 2	Data Integration Analyst / Specialist I*	per hour						
132-51	3006AT	Proces Engineer 3	Data Integration Analyst / Specialist II*	per hour						
132-51	3006AU	Proces Engineer 4	Data Integration Analyst / Specialist III*	per hour						
132-51	3006AV	Systems Engineer 4 EGM	Sensor Integration / Operations Manager	per hour						
132-51	3006AX	Systems Engineer 1	Sensor Integration / Operations Specialist I*	per hour						
132-51	3006AY	Systems Engineer 3	Sensor Integration / Operations Specialist II*	per hour						
132-51	3006AZ	Systems Engineer 4	Sensor Integration / Operations Specialist III*	per hour						
132-51	3006BA	Training Developer 4	Governance, Training and Policy Manager	per hour						
132-51	3006BB	Training Developer 2	Governance Training and Policy Specialist I*	per hour						
132-51	3006BC	Training Developer 2.5	Governance Training and Policy Specialist II*	per hour						
132-51	3006BD	Training Developer 3	Governance Training and Policy Specialist III*	per hour						
132-51	3006BE	IA-Security Engineer 4	Data and System Security Manager	per hour						
132-51	3006BF	IA-Security Engineer 1	Data and System Security Analyst / Specialist I	per hour						
132-51	3006BG	IA-Security Engineer 2	Data and System Security Analyst / Specialist II*	per hour						
132-51	3006BH	IA-Security Engineer 3	Data and System Security Analyst / Specialist III*	per hour						
			* for purposes of labor categories, a level "I" is the most junior, least experienced resource, while a level "III" is most senior, and most experienced.							

CDM CMaaS Labor Categories and Rates
CDM CMaaS Labor - Option Year 4

Technica®

SIN	CLIN	Offeror's GSA Schedule 70 Labor Category	CMaaS Labor Category	Rate Unit	CMaaS BPA Government Site Rate	CMaaS BPA Contractor Site Rate	Offeror's GSA Schedule Holder Rate (Gov. Site)	Offeror's GSA Schedule Holder Rate (Contractor Site)	% Discount CMaaS BPA / GSA Schedule 70 Rate (Gov. Site)	% Discount CMaaS BPA / GSA Schedule 70 Rate (Contractor Site)
	4006		CMaaS Labor Category	per hour	(b) (4)					
132-51	4006AA	Project Mgr-Technical 4	Integration Services Project Manager Senior	per hour						
132-51	4006AB	Project Mgr-Technical 2	Integration Services Project Manager Junior	per hour						
132-51	4006AC	IA-Security Engineer 4	Integration Services Subject Matter Expert I*	per hour						
132-51	4006AD	IA-Security Engineer 5	Integration Services Subject Matter Expert II*	per hour						
132-51	4006AE	Corporate Consultant	Integration Services Subject Matter Expert III*	per hour						
132-51	4006AF	Subject Matter Expert 6	Integration Services System Architect	per hour						
132-51	4006AG	Computer Programmer 1	Integration Services System Programmer I*	per hour						
132-51	4006AH	Computer Programmer 2	Integration Services System Programmer II*	per hour						
132-51	4006AI	Computer Programmer 3	Integration Services System Programmer III*	per hour						
132-51	4006AJ	Systems Analyst 2	Integration Services Hardware/Software Specialist I*	per hour						
132-51	4006AK	Systems Analyst 2.5	Integration Services Hardware/Software Specialist II*	per hour						
132-51	4006AL	Systems Analyst 3	Integration Services Hardware/Software Specialist III*	per hour						
132-51	4006AM	Test Engineer 3	Integration Services Quality Assurance / Test Manager	per hour						
132-51	4006AN	Quality Assurance Specialist 1	Integration Services Quality Assurance Analyst I*	per hour						
132-51	4006AO	Quality Assurance Specialist 2	Integration Services Quality Assurance Analyst II*	per hour						
132-51	4006AP	Quality Assurance Specialist 3	Integration Services Quality Assurance Analyst III*	per hour						
132-51	4006AQ	Proces Engineer 4	Integration Services Change Management Lead	per hour						
132-51	4006AR	Proces Engineer 4 EGM	Data Integration Manager	per hour						
132-51	4006AS	Process Engineer 2	Data Integration Analyst / Specialist I*	per hour						
132-51	4006AT	Proces Engineer 3	Data Integration Analyst / Specialist II*	per hour						
132-51	4006AU	Proces Engineer 4	Data Integration Analyst / Specialist III*	per hour						
132-51	4006AV	Systems Engineer 4 EGM	Sensor Integration / Operations Manager	per hour						
132-51	4006AX	Systems Engineer 1	Sensor Integration / Operations Specialist I*	per hour						
132-51	4006AY	Systems Engineer 3	Sensor Integration / Operations Specialist II*	per hour						
132-51	4006AZ	Systems Engineer 4	Sensor Integration / Operations Specialist III*	per hour						
132-51	4006BA	Training Developer 4	Governance, Training and Policy Manager	per hour						
132-51	4006BB	Training Developer 2	Governance Training and Policy Specialist I*	per hour						
132-51	4006BC	Training Developer 2.5	Governance Training and Policy Specialist II*	per hour						
132-51	4006BD	Training Developer 3	Governance Training and Policy Specialist III*	per hour						
132-51	4006BE	IA-Security Engineer 4	Data and System Security Manager	per hour						
132-51	4006BF	IA-Security Engineer 1	Data and System Security Analyst / Specialist I	per hour						
132-51	4006BG	IA-Security Engineer 2	Data and System Security Analyst / Specialist II*	per hour						
132-51	4006BH	IA-Security Engineer 3	Data and System Security Analyst / Specialist III*	per hour						
			* for purposes of labor categories, a level "I" is the most junior, least experienced resource, while a level "III" is most senior, and most experienced.							